PRIVACY MANUAL FOR DENTAL PRACTICES 2014

Resources to aid compliance with Federal Privacy, eHealth and State Health Records legislation.

KINDLY SPONSORED BY:

With over a decade of experience providing insurance for the specific needs of the dental profession, Guild Insurance Limited is honoured to sponsor the production of the 2014 Privacy Manual for Dental Practices.

ADAVB Inc. PRIVACY MANUAL FOR DENTAL PRACTICES

INDEX

March 2014

Dear Member,

ADAVB PRIVACY MANUAL FOR DENTAL PRACTICES

ADAVB is pleased to announce that the ADAVB Privacy Manual for Dental Practices has been updated to reflect changes to the Privacy Act 1988 (Cth) which commence operation on 12 March 2014.

Amendments to the Privacy Act have introduced the "Australian Privacy Principles" or "APPs" which replace the "National Privacy Principles" (NPPs). Private dental practices across Australia must now comply with the new APPs.

In particular, members should be aware that the APPs have significantly changed privacy obligations for dental practices including in areas of:

- direct marketing;
- overseas disclosure of personal information (for example "cloud" storage); and
- the handling of unsolicited information.

In addition, dental practices must now have a clearly expressed and up-to-date privacy policy that sets out how the practice manages personal information (including health information). The policy must be reasonably available free-of-charge.

The manual contains a range of material (including a privacy policy) that will assist practices in meeting their obligations under the APPs and applicable State legislation.

Other new areas covered by the Manual include the Personally Controlled Electronic Health Record (PCEHR) and Individual Healthcare Identifiers (IHIs).

In an important development, the manual has also been amended to take into account Tasmanian law and as such, it can now be used by Tasmanian practices.

The revised Manual can be accessed at www.adavb.org or a bound copy or CD may be purchased via the enclosed order form.

We trust you will find this manual a valuable membership service. Please let us know if you have any questions or comments.

Yours sincerely

Garry Pearson
Chief Executive Officer

Level 3, 10 Yarra Street South Yarra VIC 3141 | PO Box 9015 South Yarra VIC 3141
P 03 8825 4600 F 03 8825 4644 E pp@adavb.net W www.adavb.net

Instructions for Using the Privacy Manual for Dental Practices

This Privacy Manual for Dental Practices has been prepared by the ADAVB Inc to assist Members in addressing their obligations under the Privacy Act 1988 (Cth), the Victorian Health Records Act 2001 for Victorian Practitioners and the Charter of Health Rights and Responsibilities for Tasmanian practices.

No doubt some practices may have particular issues that have not been or have only partially been addressed. The Privacy Manual cannot be all things to all practices and needs to be treated as a guide. Additional privacy materials are published by the Office of the Australian Information Commissioner, the Tasmanian Health Complaints Commissioner and the Victorian Health Services Commissioner.

If you are responding to a complaint, you should consider advice from your professional indemnity insurer.

Members may find it useful to approach the kit using the 12 steps outlined over the page.

Practices should develop systems and processes that are designed to protect patients' privacy. With the advent of electronic health records and digital communication, more than ever it is imperative that patient privacy is protected.

Templates are provided for you to add relevant information, however we recommend you do not delete words which have been included to address your legal compliance obligations.

DISCLAIMER

The information contained in this Privacy Manual is provided only as a general guide to ADAVB members in relation to their response within their dental practices to privacy laws applicable to private dental practices located in Victoria and Tasmania.

The ADAVB and authors are in no way responsible for the loss or liability by anyone acting solely on the basis of information in this Manual or for any error in or omission from it.

COPYRIGHT

STEP 1.	Read the ***Overview of Privacy (Section 1)***, and familiarise yourself with the ***Extracts from the Privacy Act and, as applicable the Health Records Act and the Charter of Health Rights and Responsibilities (Appendices 1, 2 and 3)***.	
STEP 2.	Read the ***Frequently Asked Questions (Section 3)*** and note areas specific to your practice's current needs. Undertake follow up in those areas identified.	
STEP 3.	Appoint a Privacy Officer for your practice.	
STEP 4.	Undertake the practice ***Privacy Action Checklist (Section 4.1.1)*** and commence working through the checklist to its completion. Record your findings.	
STEP 5.	***The Practice Privacy Policy*** ***(Section 4.1.3)***	Ensure the Privacy Policy is easily available to patients, including placement on the practice website.
	The Notice for Patient Information ***(Section 4.1.3.1)***	Display in a prominent place in Waiting Room or at Reception.
STEP 6.	Undertake a privacy audit of your practice by using **(*Section 4.1.5).***	
STEP 7.	Following the audit, ensure that appropriate actions are taken to address the findings of the audit, i.e: if more people have access to the personal information than have a need to have access; or if patients do not know why any or all of the information collected is necessary; then remedial steps will need to be introduced. Identify those steps and commence working through them.	
STEP 8.	In terms of specific records ***(Sections 4.1.6 and 4.1.7)*** may assist in your practice better **managing its records.**	
STEP 9.	Ensure staff are familiar with the ***Practice Privacy Provisions (Section 4.3.1)*** and sign the ***Undertaking (Section 4.3.2).***	
STEP 10.	All staff and contractors must understand and have easy access to the ***Practice Privacy Handling Framework (Section 4.3.3)***.	
STEP 11.	Train staff on the ***Practice Privacy Complaints Register*** and ensure it is in a secure place and available as and when required for use. See **(*Section 4.3.4)*** for Register.	
STEP 12.	Inform staff of the practice requirements under the Privacy legislation concerning **Employee Records**. A copy of **(*Section 4.3.5)*** can be personally given to existing and new staff to ensure their understanding of Privacy's application to personnel records.	

OVERVIEW OF PRIVACY

Introduction

Dentists and dental practices in Victoria are subject to both State and Federal privacy laws.

In Tasmania, private dental practices are subject to the Federal Privacy Act. There is no specific Tasmanian legislation dealing with privacy in the private sector; however, private dental practices in Tasmania are bound to comply with the Charter of Health Rights and Responsibilities (**Charter**) which sets out a number of patient rights concerning confidentiality and privacy.

Although the Federal and State regulatory schemes differ, each contains broadly similar provisions and in general, compliance with the Federal Privacy Act will ensure compliance with State-based obligations.

Practitioners must also note that in both jurisdictions there are common ethical and professional obligations concerning patient privacy and confidentiality.

Health Records Act 2001

The *Health Records Act 2001* (Victoria) (**the HRA**) commenced operation on 1 July 2002.

The HRA aims to protect health information handled within the Victorian public and private sectors. It also provides individuals with a right to access their health information held by a private sector health organisation (such as private dental practices).

Under the HRA, "Health information" is defined to include information or an opinion about the physical, mental or psychological health of an individual, and can include other identifying information collected in providing an individual with a health service.

Under the HRA, health information that is collected, held or used by health providers must be handled in accordance with 11 Health Privacy Principles.

The Health Services Commissioner of Victoria administers the HRA. Complaints regarding a breach of the HRA can be made to the Health Services Commissioner.

Privacy Act 1988

The *Privacy Act 1988* (Commonwealth) (**the Privacy Act**) covers the handling of personal information (including health information) by Federal government organisations, credit reporting organisations and certain private sector organisations.

In general, the Privacy Act does not apply to small businesses; however, if the business holds health information, then the Privacy Act applies regardless of the size of the business.

Prior to March 2014, the National Privacy Principles (**NPPs**) regulated how personal information (including health information) was to be handled under the Privacy Act. From 12 March 2014, the NPPs were replaced with the Australian Privacy Principles (**APPs**). **All dental practices in Australia must comply with the APPs.**

A breach of privacy under the Privacy Act can give rise to a complaint to the Office of the Australian Information Commissioner (**OAIC**).

Tasmanian Charter of Health Rights and Responsibilities

The Charter of Health Rights and Responsibilities (**Charter**) was introduced in 1999 in accordance with the *Health Complaints Act 1995* (Tas).

Health service providers in Tasmania (such as dental practitioners and practices) must provide care that is consistent with the Charter. A patient may complain to the Health Complaints Commissioner if a health service provider acts in manner that is inconsistent with the Charter.

The Charter contains a number of rights and responsibilities of health service providers and patients under the following headings:

- active participation in health care;
- individualised service that is free from discrimination;
- confidentiality, privacy and security;
- access to complaints mechanisms;
- carers;
- contribution of health service providers.

Under Federal and State laws, organisations must document their privacy policies and procedures. This manual offers a range of resources to assist staff in member practices to comply with both Federal and State privacy legislation.

The Australian Privacy Principles

The Australian Privacy Principles (**APPs**) are contained in Schedule 1 of the Privacy Act.

The APPs set out how an "APP entity" is to handle personal and health information. For the purposes of the Privacy Act, dental practices are "APP entities".

A summary of the 13 APPs follows:

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 – for example if giving individuals the option is impracticable.

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 which includes health information and genetic 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 APP entity 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 APP entity 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.

Further Information

For further information about the Federal Privacy Act and other APP resources, refer to the Office of the Australian Information Commissioner's website at www.oaic.gov.au.

Victorian Health Privacy Principles

Victorian dental practices should note that Schedule 1 of the *Health Records Act 2001* sets out the Health Privacy Principles (HPPs) which relate to the collection, use, disclosure, quality, security, retention and transfer of, and access to, 'health information'.

There are 11 HPPs, that are very similar to the APPs in terms of their scope. In summary the HPPs are as follows:

HPP 1 - governs the **collection** of health information. It provides that organisations may only collect health information:

- with the patient's consent, or
- if the patient is incapable of giving consent but it is necessary to provide the information to another health service for the purpose of providing further necessary health services to the individual.

HPP 2 - governs the **use and disclosure** of health information. Generally speaking an organisation may only use the information for the purpose it was collected, although there are some public interest exceptions.

HPP 3 - provides that the health provider must take steps to ensure that the health information it collects and uses is **up-to-date and relevant** to its function and activities.

HPP 4 - organisations must have reasonable **security** systems in place to protect health information they have collected from misuse, loss, unauthorised access or disclosure. HPP 4 also requires health records to be maintained for specified periods depending on whether the record is that of a child or an adult.

HPP 5 - requires organisations to set out in documentary form clear **policies** as to how it manages health information as collected and what steps an individual must take to access it.

HPP 6 - provides individuals with the right of **access** to records concerning them that are held in the private sector and their rights to collect it or update it. The provisions are similar to the provisions in the Freedom of Information Act 1982 granting individuals who are patients of public sector organisations to access and amend records about them.

HPP 7 - restricts the use of **identifiers** (e.g. Medicare numbers) without the patient's consent.

HPP 8 - where lawful and practicable, preserves the right of individuals to remain **anonymous**.

HPP 9 - limits **transfer** of health information outside the State without the patient's consent.

HPP 10 - regulates what organisations must do with their records when the business is **sold, transferred, amalgamated or closed down.** A related Statutory Guidelines dictates what advice must be given to patients in these circumstances.

HPP 11 - grants individuals the right to have records about their **treatment transferred** from one health service provider to another.

The complete HPPs and APPs are reproduced in appendices 1 and 2 of this manual.

A comparison between the APPs and the old NPPs is set out in the document:
"Australian Privacy Principles and National Privacy Principles – Comparison Guide
Summary and analysis of key differences for organisations" which is available on the website of the Office of the Australian Information Commissioner (www.oaic.gov.au)

Tasmanian Charter of Health Rights and Responsibilities

Tasmanian dental practices should note the following excerpt of "RIGHT 3 - CONFIDENTIALITY, PRIVACY AND SECURITY" from the Charter.

The Rights of the Health Service Consumer

- The health service consumer has the right to have his/her personal health information and any matters of a sensitive nature kept confidential.

  No identifying information about the consumer, his/her condition or treatment may be disclosed without his/her consent unless the disclosure is required or authorised by law.

  In some cases, the provider is legally required to disclose health issues under mandatory reporting requirements or in the public interest.

- The right to be informed if the provider is required to disclose information about his/her health due to mandatory reporting requirements or in the public interest.

- The right to know who may have access to his/her personal health record, within the bounds of confidentiality.

- The right to know what sort of information is kept on his/her health record.

- The right to nominate another person who may receive information about the consumer's health status and care. This person does not necessarily have to be a next of kin.

- The right to have information about his/her health status and care passed on to another provider, at his/her request.

- The right to expect that staff of health service facilities are bound by confidentiality agreements, and will be disciplined if these agreements are breached.

- The right to health service facilities which ensure his/her privacy when receiving health care.

- The right to be treated with sensitivity as regards his/her confidentiality and privacy.

- The right to expect that information about his/her health is kept securely and cannot be easily accessed by unauthorised persons.

- Any record that contains personal information about the consumer's health should not be left in reception areas or treatment rooms. When the provider or another authorised person does not have a file, it should be stored securely. The same applies to computer or electronic records.

- Similarly, health service providers should not talk about consumer's health or care where other unauthorised persons can overhear them.

The Rights of the Health Service Provider

- The provider has the right to discuss the health care and treatment of a consumer with other providers for advice and support, in the best interest of the consumer's health and well-being.

Enforcement

An individual concerned about a breach of the HPPs can make a complaint to the Victorian Health Services Commissioner (**HSC**).

Complaints regarding a breach of the APPs can be made to the Office of the Australian Information Commissioner (**OAIC**).

Complaints concerning a breach of the Tasmanian Charter of Health Rights and Responsibilities (**Charter**) can be made to the Tasmanian Health Complaints Commissioner.

Complaints concerning a breach of either the APPs or the HPPs could give rise to a compensation claim. The Tasmanian Health Complaints Commissioner has no power to award compensation; however, compensation settlements can be negotiated if a health provider has breached the Charter.

A registered practitioner in breach of the APPs, HPPs or the Charter could also have a complaint made against them to the Dental Board of Australia.

Under the Health Records Act, penalties may apply in certain situations; for example where health information is damaged or destroyed to frustrate a patient's access to their information.

From March 2014, serious or repeated breaches of the Privacy Act (including a breach of the APPs) can give rise to penalties of up to $340,000 in the case of individuals and $1.7m in the case of companies.

At a minimum, Victorian dentists and their staff must handle patient information in accordance with the APPs and the HPPs.

Tasmanian practitioners and their staff must comply with the APPs and the Charter.

In both jurisdictions however, compliance with the APPs will generally result in compliance with the HPPs and the Charter.

Details about the complaints processes are set out in the websites of the:

- Office of the Australian Information Commissioner (www.oaic.gov.au);
- The Victorian Health Services Commissioner (www.health.vic.gov.au/hsc); and
- The Tasmanian Health Complaints Commissioner (www.healthcomplaints.tas.gov.au).

Alleged or potential breaches of privacy laws are generally reportable as a notifiable event under professional indemnity insurance. Practices and practitioners must ensure that they contact their insurer or ADAVB if contacted by the Victorian Health Services Commissioner, the Tasmanian Health Complaints Commissioner, the OAIC or if the practitioner or practice believes a privacy breach may have occurred.

Further Information

- For more information about the Health Records Act, refer to **www.health.vic.gov.au/hsc**
- For more information about the Federal Privacy Act, refer to **www.oaic.gov.au.**

- For more information about the Charter, refer to www.healthcomplaints.tas.gov.au.

The Personally Controlled Electronic Health Record

The National E-Health Transition Authority Limited (known as NEHTA) was established by the Australian, State and Territory Governments to develop better ways of electronically collecting and securely exchanging health information.

E-Health is an integral part of the Australian Government's agenda for health reform. As such, the 2010/11 Federal Government budget included a $466.7 million investment over 2 years for a national Personally Controlled Electronic Health Record (PCEHR) system for all Australians.

To this end, the *Personally Controlled Electronic Health Records Act 2012* (Cth) and the *Personally Controlled Electronic Health Records Regulation 2012* (Cth) (the PCEHR legislation) commenced operation on 29 June 2012.

As of 1 July 2012, Australians have been able to choose to register for a PCEHR.

The intended benefits of the PCEHR system for individuals include:

1. access: individuals will be able to access key pieces of their health information;

2. improved healthcare: an availability of a wider source of health information will lead to opportunities for improved prevention, early intervention and treatment of chronic diseases, as well as improved diagnosis and treatment in emergencies;

3. informed healthcare choices: individuals will be able to access their own PCEHR, view their records and in time, may link to health literacy information relating specifically to their needs.

Organisations such as dental practices are able to apply for registration as a 'healthcare provider organisation' to access the PCEHR. In doing so, the organisation must agree to the conditions of registration contained in the PCEHR legislation and agree to enter into and remain a party to a participation agreement with the Secretary of the Department of Health and Ageing of the type contained in the *PCEHR Rules 2012* (Cth).

The PCEHR Rules also set out a number of requirements which must be satisfied in order for an organisation to be eligible and remain eligible, for registration as a healthcare provider organisation. This includes having a written policy addressing the matters specified in the PCEHR Rules and employing reasonable user account management practices.

Those conditions in the PCEHR legislation include certain requirements for uploading records. The conditions also include the requirement that an organisation does not discriminate in providing healthcare to a consumer, because the consumer does not have a PCEHR.

Significantly, the PCEHR legislation contains certain sanctions for unauthorised collection, use or disclosure of health information included in a consumer's PCEHR. Significant penalties may apply.

To participate in the PCEHR, dental practices must comply with a number of obligations including an obligation to develop, maintain, enforce and communicate to staff written policies relevant to the eHealth record system to ensure that the practice's use of the system is secure, responsible and accountable.

The policies need to deal with a range of matters, including authorising persons within the practice to access the system, training, and physical protection of IT systems.

Although the PCEHR is likely to become an increasingly important tool in the delivery of health care across Australia, dental practitioners are reminded that:

1. the PCEHR is not a replacement for existing clinical records, nor will it replace the need for practitioners to keep their own clinical records. At best, the PCEHR will be a summary of a patient's health information;

2. although the information contained in the PCEHR may be accessible to other practitioners treating a patient;

    a. it does not relieve a dentist of making independent clinical decisions in the patient's treatment; and

    b. it does not replace direct (point-to-point) communication between other practitioners who may be providing care to the patient; and

3. there is no guarantee that the information contained in the PCEHR is current, accurate or complete or that an individual practitioner has access to all information contained in a patient's PCEHR. Practitioners must always ensure they obtain up-to-date clinical information from the patient at the time of presentation/treatment.

A further aspect of the PCEHR system is the introduction of unique Healthcare Identifiers for all Australians.

Specific privacy laws apply in relation to these Healthcare Identifiers which must only be used for authorised purposes. Authorised purposes include where the use or disclosure of a Healthcare Identifier is part of the provision of healthcare to the patient, and where the use or disclosure is authorised under another law (for example where disclosure is required under a court issued subpoena). Healthcare Identifiers must not be used or released for an unauthorised purpose. Penalties of up to two years imprisonment, a fine of $20,400, or both apply. If a body corporate such as an incorporated dental practice is convicted of using or releasing a patient's Healthcare Identifier for an unauthorised purpose, a court may impose a fine of up to $102,000. Unauthorised purposes for the use or disclosure of a Healthcare Identifier include where it is used or disclosed in relation to employing a patient.

ABOUT DENTAL RECORDS

The ADAVB advises its members that records should be accurate, contemporaneous, legible, comprehensible, and address medical issues which may have occurred, or are relevant in the management of a particular case.

The Dental Board of Australia has published guidelines (**Guidelines**) on dental records.

The Guidelines provide that practitioners must create and maintain dental records that serve the best interests of patients and that contribute to the safety and continuity of their dental care.

The Guidelines describe minimum requirements for dental records whether they are in paper-based or electronic form.

Practitioners must also be familiar with the "Code of Conduct for Registered Health Practitioners" (**Code**) published by the Dental Board of Australia which also contains provisions regarding health records.

The Guidelines and the Code are available at http://www.dentalboard.gov.au.

1. The nature of dental records

The clinical record of a patient may consist of all of the following:

a) Up-to-date medical history - preferably signed and dated by the patient.
b) Clinical Notes (electronic or hard-copy). The date, diagnosis and treatment notes every treatment, with full details of any referrals or any incidents, episodes or discussions that have a direct bearing on the patient's treatment or care.
c) Monitoring information such as BPE/CPITN scores, periodontal probing depths and other indices, tracking of oral pathology and other conditions.
d) Results of investigations (Pathology Reports, etc).
e) Records of financial transactions, quotes and estimates made by the patient.
f) All contact with, and correspondence to and from the patient, or any third party (consultant, other dentists, doctor etc) and details of anyone contributing to the patient record.
g) Consents obtained and warnings given.
h) Findings/diagnosis on radiographs - particularly if discovered after the patient has left the surgery. Radiographic tracings, pre and post-treatment photographs, and Intra-Oral Camera Images.
i) Drugs administered, prescribed or supplied and dosages and quantities (as required under the Victorian Drugs Poisons and Controlled Substances Regulations 2006 – reviewed 2012).
j) Plaster casts and models of teeth.
k) Instructions and communication with laboratories.
l) Anything else the dentist considers to be relevant or that records identifiable information about a patient.

Practitioners must also be mindful that not all dental records can be reduced to either a “database” (see Computerised Records below) or a simple paper file.

Other practice records required for compliance purposes, but not necessarily related to a particular patient’s treatment, include:

- Autoclave print outs, data cards, log books and service records
- Service records for radiographic equipment
- Occupational Health and Safety records
- Up to date Systematic Operating Procedures for Infection Control (refer to the ADAVB SOP Manual)

2. Obligation to maintain “good records”

The rationale for keeping contemporaneous and accurate clinical records is to ensure another practitioner can read the record and know exactly how and why a patient has been treated in a particular way.

Courts recognise that clinical records are not taken for the purpose of defending legal claims and therefore place considerable weight on contemporaneous clinical records as a record of what occurred on a particular day that is not influenced by subsequent events (including legal action).

Because of this, a well-documented health record is the greatest aid in defending litigation, and a Court will generally prefer the evidence contained in contemporaneous clinical records.

However, the converse is also true, and in the absence of good clinical notes, a practitioner’s version of events can be difficult (sometimes impossible) to prove or explain.

Inadequate clinical notes will be particularly problematic for a practitioner if there is no evidence to justify a course of treatment, including the prescription or administration of medication.

Practitioners are reminded that later amendment of a record should be avoided unless there is a complete explanation of the reasons for such action and retrospective notes are identified as such in the record. Although retrospective notes may be added, practitioners should never tamper with notes in an attempt to “fix” them on notification of a complaint or legal action, as such tampering will render the record useless as evidence and criminal penalties may apply if notes are destroyed.

3. Computerised Records

Many practices rely on computerised records.

The risks inherent in computerised records are that:

- If there is a privacy breach, all records held by a practice could be accessed;

- If there is a system failure, all practice data including all patient records and appointment records could be lost.

For this reason, practices must adopt sophisticated policies and procedures regarding their computerised records.

For example, practices should consider:

- Data security (authenticating the user with a unique secure password, restricted access to information, audit trails etc.);
- Data integrity;
- Accessibility (back-up and recovery, transfer of data, rate of retrieval etc.);
- System integration and interaction;
- Data volume; and
- The practicalities of log-ins, automatic log-offs after inactivity etc.
- Disaster Recovery Plan

Practices should be particularly cautious when lap-tops and other mobile devices containing clinical records are taken off-site or if removable storage devices, such as USB drives are used to store and transport clinical records. See also Mobile Device Policy.

Practices should have sufficient security controls in place regarding access to electronic records and the practice computer system.

Because of security issues regarding transmission of information by email, practices should be cautious of using email as a means of communicating clinical information. Unless appropriate security measures are in place, it may not be appropriate to send a patient's clinical file by email. Consideration should be given to using encrypted email or attachments.

Post records securely – use Registered Mail or Express Post (ADA Policy Statement 5.17).

Creation of electronic records

There are various ways in which electronic records can be created, which include imaging (scanning) clinicians' notes, uploading digital information and direct entry of patient information at the point of care, or a combination of the above. Any electronic recording may require the bar coding of patients' names (assigning a unique identifier), to prevent records being attributed to the wrong patient.

Practitioners should be mindful of limitations of data entry options that restrict a clinician's ability to record individualised patient notes, for example structured entry systems may confine practitioners to a set of standard entries that may be not suitable in all situations.

In the past, electronic records were not easily accepted by courts. However, this has now changed, and across Australia, electronic records have the same evidentiary weight as hard-copy records.

However, although electronic records may be admitted as evidence, the reliability and accuracy of electronic records can still be questioned – particularly in relation to access and amendment of the record. For this reason it is important to consider

how an information management system is designed, with attention to security, operational maintenance and operation logs (including exception management logs).

Regular system audits should be conducted and secure off-site backup must be considered.

Cloud storage

The recent emergence of "cloud" computing means that clinical records could be stored in off-site systems. Practices using such data warehousing must ensure that appropriate security measures are in place and that the APPs and HPPs are complied with at all times.

In particular however, APP 8.1 provides that in relation to overseas data transfers, it is the responsibility of the transferring entity (such as the dental practice) to take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the APPs.

The effect of APP 8.1 is that if the overseas recipient acts in a manner that is in breach of the APPs then, in certain circumstances, the act done, or a practice engaged in, by the overseas recipient is taken (under section 16C of the Federal Privacy Act) to have been done, or engaged in, by the entity that transferred the data (the dental practice) and to be a breach of the APPs. In other words, the dental practice is liable for a breach by the overseas entity.

APP 8.2 provides that dental practices can avoid operation of APP 8.1 (and avoid liability for any possible privacy breach by the overseas "cloud" storage provider) if:

a. the practice reasonably believes that:

    i. the recipient of the information (the "cloud" storage provider) 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 APPs 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.

The OAIC has specified in its "Key Concepts" Guidelines, that a practice will have a "reasonable belief" if the practice applies a reasoned judgement to the circumstances at the time of making the relevant assessment.

If a practice cannot be satisfied that the requirements of APP 8.2(a) above can be met, then in general, consent of patients must be obtained before the patient's health information is transferred off-shore. That consent should comply with the requirements of APP 8.2(b).

Maintaining records

Practitioners must have appropriate IT management systems and processes in place to ensure data is not lost during system maintenance or upgrades.

Practices must ensure that legacy systems are maintained to allow continued access to records for the periods required under HPP 4 (Data Security and Data Retention) which is the later of:

- in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or
- in any case, not less than 7 years after the last occasion on which a health service was provided to the individual by the provider.

APP 11.2 provides that organisations (such as dental practices) must take reasonable steps to destroy or de-identify personal information, once it is no longer needed for any purpose for which it may be used or disclosed in accordance with the APPs:

- if it is not contained in a Commonwealth record (which is not applicable to dental records); and
- if the organisation is not required by or under an Australian law (such as the HPPs), or a court/tribunal order, to retain the information (APP 11.2(d)).

For Victorian Dentists, this means they must comply with the requirements of HPP 4 in maintaining dental records in order to comply with the requirements of APP 11.2.

For Tasmanian dentists, there is no legislation specifying that records must be kept for a particular period of time. However, the standards set out in HPP 4 represent good practice and accord with the retention periods recommended under the Guidelines and therefore, Tasmanian dentists should consider compliance with the retention periods set out in HPP 4.

Use of records in legal proceedings

All practices must be aware that a patient's health records may be used by the practice to defend claims made by the patient.

Practices must also be aware that in Victoria, criminal penalties apply if documents are destroyed or rendered illegible and the documents were to be used or were likely to be used in evidence in a legal proceeding. Possible jail terms apply.

Dentists in both jurisdictions may also wish to seek advice from their insurer regarding optimum periods for retention of records from a risk management perspective.

Other types of data

In relation to radiographs and correspondence, care should be taken scanning these types of documents. Correspondence should not be stored as text as this can be altered easily; rather, correspondence should be scanned. Radiographs that are scanned or stored electronically should be of sufficient resolution to be diagnostically relevant in future, and ideally, Digital Imaging and Communications in Medicine (DICOM) files should be stored.

4. Medicare

Practitioners who provide services for which Medicare benefits are payable must ensure their records are “adequate” and “contemporaneous”.

To be adequate for Medicare purposes, the patient or clinical record needs to:

- Clearly identify the name of the patient; and
- Contain a separate entry for each attendance by the patient for a service and the date on which the service was rendered or initiated; and
- provide clinical information adequate to explain the type of service rendered or initiated; and
- be sufficiently comprehensible that another practitioner, relying on the record, can effectively undertake the patient’s ongoing care.

To be contemporaneous for Medicare purposes, the patient or clinical record should be completed at the time that the service was rendered or initiated or as soon as practicable afterwards (on the day of the visit).

A practitioner who fails to present adequate documents when requested by Medicare may have to repay any benefits claimed and may be subject to penalties.

Part 1 – About the legislation

1. Are all dental practices covered under the privacy legislation?

*Yes. All dental practices in Victoria are covered under the Federal Privacy Act and the Victorian Health Records Act. Dental practices in Tasmania are covered by the Federal Privacy Act and are subject to the Charter of Health Rights and Responsibilities (**Charter**).*

2. What does the privacy legislation cover?

The privacy legislation (the Health Records Act and the Privacy Act) covers a wide range of information handling practices, including:

- *needing to gain consent for the collection of health information;*
- *what to tell individuals when information is collected;*
- *what to consider before passing health information on to others;*
- *the details that should be included in a dentist's Privacy Policy;*
- *securing and storing information; and*
- *providing patients with a right to access their health records.*

The Charter covers similar areas of privacy.

The privacy legislation applies to private sector or non-government organisations that provide a "health service". Dental practices provide a "health service" for the purpose of privacy legislation.

Under the Health Records Act, organisations that provide health services are referred to as "health service providers", which includes:

- *dental care providers;*
- *health services provided via the Internet (e.g. counselling, advice, medicines), tele-health and health mail order companies.*

The Federal Privacy Act refers to "APP entities" which includes most medical and dental practices operating in Australia.

The Charter is applicable to "health service providers" which specifically includes dental practices.

3. Do employees and contractors have any obligations?

Each employee and *contractor of a private or non-government organisation that provides a health service needs to be aware of their obligations, and those of the organisation under the Privacy Act and, in the case of Victorian dental practices, the Health Records Act and for Tasmanian practices, the Charter.*

4. What does the Privacy legislation apply to?

The confidentiality of patients' health information is already strongly protected in the health sector – through the obligations dentists have under professional and ethical codes of practice (including the Charter). The Privacy Act and the Health Records Act do not prevent these codes of practice from continuing to apply.

The Privacy Act and the Health Records Act both apply to "Health Information" which includes:

- *information or an opinion about:*
    - *an individual's health or disability at any time (that is, past, present or future);*
    - *an individual's expressed wishes regarding future health services;*
    - *health services provided, or to be provided, to the individual;*
- *information collected whilst providing a health service (such as a dental service); or*
- *information collected in connection with the donation or intended donation of body parts and substances; or*
- *genetic information.*

In practice, this means that "Health Information" includes any information collected by a dentist or practice staff during the course of providing treatment and care to an individual, including:

- *medical information;*
- *personal details, such as a name, address, admission and discharge dates, billing information and Medicare number;*
- *information generated by a health service provider, such as notes and opinions about an individual and their health;*

- *x-rays or other test results or reports;*
- *information about physical or biological samples, where it can be linked to an individual (for example, where they have a name or identifier attached); and*
- *genetic information, when this is collected or used in connection with delivering a health service, or genetic information when this is predictive of an individual's health.*

Under the Privacy Act, "Health Information" is a form of "Sensitive Information" and when the term "Sensitive Information" is used in the APPs or the Privacy Act, it includes a reference to Health Information.

The Personally Controlled Electronic Health Records and Individual Healthcare Identifiers

*Practices must also be aware that the use and disclosure of Individual Healthcare Identifiers (**IHI**) (unique identifiers assigned to all Australians) are governed under the Healthcare Identifiers Act 2010 (Cth). This is a federal law that applies to all health service providers (including dental practices) in Australia.*

There are also specific laws (the Personally Controlled Electronic Health Records Act 2012 and the associated Personally Controlled Electronic Health Records (Consequential Amendments) Act 2012) governing use and access to the Personally Controlled Electronic Health Record (PCEHR). Penalties apply for misuse of the PCEHR.

5. What is a "health service"?

The Privacy Act stipulates providing a "health service" includes any activity that involves:

- *assessing, recording, maintaining or improving a person's health; or*
- *diagnosing or treating a person's illness or disability; or*
- *dispensing a prescription drug or medicinal preparation by a pharmacist.*

The Health Records Act uses a similar definition, with the addition of disability, aged and palliative care services.

Dentists, in their professional practice will be providing a "health service" (both under the Privacy Act and the Health Records Act).

6. Does my practice have to comply with the APPs or the HPPs?

Victorian practices must comply with both the APPs and the HPPs. In general, complying with one set of principles will mean the practice is compliant with the other principles.

Tasmanian practices must comply with the APPs (there are no Tasmanian equivalents of the HPPs). In addition, Tasmanian practices must comply with the Charter – however, the rights contained in the Charter are reflected in the APPs – and compliance with the APPs (under the Federal Privacy Act) will ensure compliance with the Charter obligations.

For the purpose of these Frequently Asked Questions, the APPs are relied upon with reference to the HPPs or the Charter where relevant.

Appendices 1 and 2 contain extracts from the two Acts regarding the APPs and HPPs. Appendix 3 excerpts Rule 3 from the Charter concerning privacy.

7. How is the privacy legislation governed?

The APPs are found in the Federal Privacy Act and fall within the jurisdiction of the Office of the Australian Information Commissioner (OAIC). Within the OAIC there is the Australian Privacy Commissioner who deals with privacy related matters.

The OAIC investigates privacy complaints and breaches of the APPs and may:

- *investigate interferences with privacy;*
- *accept enforceable undertakings from a practice;*
- *seek civil penalties in the case of serious or repeated breaches of privacy; or*
- *conduct assessments of privacy performance of a business (such as a dental practice).*

Serious or repeated interference with the privacy (ie. a serious or repeated breaches of an APP) may result in penalties of up to $1.7m for a company and $340,000 for individuals.

The HPPs are regulated by the Victorian Health Services Commissioner. The Health Services Commissioner has broad powers to investigate breaches of the HPPs.

The Health Services Commissioner may issue compliance notices for serious, flagrant or repeated breaches of the Health Records Act. Non-compliance with a compliance notice may result in a penalty of up to $433,000 for a company and up to $86,616 in the case of an individual.

In addition, breaches of the APPs and HPPs can give rise to compensation claims.

A breach of the Charter may give rise to recommendations by the Tasmanian Health Complaints Commissioner. A failure to respond to recommendations can give rise to a penalty of $6,500.

Individual Healthcare Identifiers

Under the Healthcare Identifiers Act 2010, health service providers (such as dentists and dental practices) in any State can only use or disclose an IHI for a purpose permitted under the Healthcare Identifiers Act that is, to communicate or manage health information as part of:

- *the provision of healthcare to the patient;*
- *the management (including investigating or resolving complaints), funding, monitoring or evaluation of healthcare;*
- *the provision of medical indemnity cover for a healthcare provider;*
- *the conduct of research that has been approved by a Human Research Ethics Committee;*

- *lessening or preventing a serious threat to an individual's life, health or safety or to public health or safety; or*

- *purposes authorised under another law. For example, a dentist may be required under a law of Victoria or Tasmania to disclose an individual's IHI in response to a subpoena.*

The use or disclosure of an IHI for an unauthorised purpose is an offence with penalties of up to $102,000 in the case of a company, and up to two years imprisonment or a fine of $20,400, or both for individuals.

For example, using an individual's IHI as part of recruiting that individual would breach the Healthcare Identifiers Act 2010.

Practitioners must be aware that a breach of the Healthcare Identifiers Act 2010 is an interference with privacy and a breach of the Privacy Act. This means that if a staff member uses or discloses an IHI for an unauthorised purpose, that individual may have committed an offence – but the practice may still be accountable for the breach of privacy.

The OAIC has jurisdiction over misuse of IHIs.

<u>Professional Reminder</u>

If you are contacted by the OAIC, the Health Services Commissioner or the Health Complaints Commissioner about an alleged interference with privacy or a breach of privacy (including misuse of IHIs) and you are insured by Guild Insurance Ltd. you should immediately contact ADAVB on 03 8825 4600 for assistance.

Practitioners are reminded that an alleged interference with privacy or a breach of privacy is a notifiable event under the professional indemnity insurance policy arranged through ADAVB and ADATas.

Part 2 – Collection Issues (HPP1/APP2, APP3, APP4, APP5)

8. What should a dental practice tell a patient when it collects health information from them?

APP 5 provides that at or before the time or, if that is not practicable, as soon as practicable after, an APP entity (such as a dental practice) 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.

APP 5.2 sets out the following matters about which an individual must be notified or otherwise made area of:

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.

See page 7 in Section 4.1.3 for a sample Patient Notice.

9. Are there limits to collecting information?

Information collected should be limited to what is necessary for the dentist's functions and activities.

In assessing what is "necessary", professional practice standards and obligations will be relevant. See Section 2 of this Manual for a discussion on dental records. Practitioners should also refer to the Code of Conduct and Guidelines on dental records published by the Dental Board of Australia.

APP 3.5 states that personal information must be collected "only by lawful and fair means". In general the concept of "fair" extends to the obligation not to use "unreasonably intrusive" means of collection.

For example, in one case dealt with by the Australian Privacy Commissioner, a patient challenged the need for a medical practitioner to retain a digital photograph of the patient in the patient's clinical record. The practitioner conceded that it was not necessary to record a digital photograph of the patient to provide a health service. The practitioner agreed to remove the photograph and to cease the practice of taking patients' photographs. (M v Health Service Provider [2007] PrivCmrA 15).

10. Are there occasions when health information can be collected without consent?

The HPPs and APPs recognise that health information may be collected without the consent of the patient. This could occur where information is received from or about a third party or if the information is otherwise unsolicited.

Under the Privacy Act, where unsolicited personal information is received by an organisation such as a dental practice:

- *an organisation must determine whether it could have collected the information under APP 3 (see APP 4.1);*
- *if the information could have been collected, then APPs 5 to 13 apply to the information (see APP 4.4); and*
- *if the organisation could not have collected the information, it must destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so (see APP 4.3).*

In general however it is possible for a dental practice to collect personal information without that person's consent if a "permitted health situation" exists in relation to that information.

Under the Privacy Act, a "permitted health situation" exists in relation to the collection by an organisation of health information about an individual if:

> *a. the information is necessary to provide a health service to the individual; and*
>
> *b. either:*
>
> > *i. the collection is required or authorised by or under an Australian law (such as the Health Records Act); or*
> >
> > *ii. the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.*

An APP entity that is 'authorised' under an Australian law (such as a Victorian law or a Tasmanian law) will have discretion under that law as to whether it will handle information in a particular way. Where a law authorises an act or practice, an entity is permitted to take the action, but it is not compelled to do so. Words such as 'may' could indicate an authorisation.

For example, the Health Records Act (HPP1) contemplates collection of information from a 3rd party and provides (at HPP 1.5) that:

> *If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is or has been made aware of the matters listed in HPP 1.4 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 or would involve the disclosure of information given in confidence.*

For the purposes of the Privacy Act, the Australian Privacy Commissioner has released a determination (Public Interest Determination No. 12) permitting health practitioners to collect health information about third parties (for example health information about family members) and has accepted that in relation to this information, individual health assessment, diagnosis and care could be compromised if the collection is not permitted.

In making the determination, the Australian Privacy Commissioner noted that requiring health and medical professionals to notify third parties of the collection of relevant health information, or to seek their consent, would delay the healthcare delivery process in individual cases, and if third party consent were routinely required, individual health care may be compromised where third parties do not provide consent.

11. What does the patient need to know?

Patients must be given certain information at the time of collecting information (or as soon as possible after). The information that must be provided is set out in Question 8 above.

The APPs also require practices to have a clearly expressed and up-to-date privacy policy setting out how the practice manages health information. See question 32 below and page 7 in Section 4.1.3 for a sample Notice for Patient Information.

<u>Professional considerations</u>

In addition to privacy obligations, there are professional considerations on what patients need to know in relation to their care. Practitioners should refer to the Code of Conduct published by the Dental Board of Australia about their professional obligations.

12. In collecting family information do you require family members' consent?

The Australian Privacy Commissioner has taken the view that the practice of collecting patients' family, social and medical histories for diagnosis, treatment and care – without the need to obtain third parties' consent – is widespread, considered best clinical practice, and is generally known and accepted in the community. In addition, the Australian Privacy Commissioner has determined that it may not be necessary in the circumstances to notify a family member that information has been collected about them. (See Public Interest Determination No. 12)

As discussed in question 10 above, under the APPs, the collection of third party information without consent is permissible if a "permitted health situation" exists.

HPP 1.5 also contemplates that an organisation such as a dental practice may collect health information about an individual from someone else, provided that it takes any steps that are reasonable in the circumstances to ensure that the individual is made aware of the collection, except where disclosure of the collection would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence.

For the purposes of the Privacy Act, Public Interest Determination No. 12 (discussed in question 10 above) provides that collection of a 3rd party's family, social or medical history is permitted if the collection is necessary for the health provider to provide a health service directly to their patient.

13. Do all our patients have to acknowledge and sign our practice policy on privacy matters?

No, it is not mandatory for patients to sign such a statement and there is nothing under the APPs or the HPPs that require such a procedure.

However, under both the APPs and the HPPs, practices must (where it is reasonable to do so) ensure relevant information is given, or is available to patients at the time of the collection (or as soon as possible thereafter). See question 11 above.

In addition, the APPs require that the practice privacy policy should be freely available to patients – such as including the policy on the practice website. See question 11 above.

Practitioners are reminded that privacy legislation should build on best practice and in general, the use or disclosure of health information should, where clinically appropriate, be discussed with the patient, particularly if the patient's information is to be used for a purpose that is not related to the patient's treatment (for example use of information for research purposes).

Part 3 – Use and disclosure issues (HPP2/ APP6 and APP7)

14. What is the significance of consent?

Consent is relevant to many decisions about how health information is collected, used or disclosed. However, express consent for use of a patient's information is not required in all situations.

The Privacy Act contemplates that consent may be "express consent" or "implied consent".

The key elements to consent are:

- *it must be provided voluntarily;*
- *the patient must be adequately informed; and*
- *the patient must have the capacity to understand, provide and communicate their consent.*

As set out in question 11 above, patients must be given certain information at the time of or as soon as practicable after information is collected. The information provided must comply with the APPs and HPPs and the provision of this information will, in part, satisfy the requirement that patients be adequately informed.

However, practices must ensure that if a patient has particular questions or concerns about the collection and use of their information, that these questions or concerns are addressed. Practices must also ensure that patients understand information given to them about the collection of personal or health information. If appropriate, consideration should be given to using interpreters or having the practice privacy policy and collection statements available in languages commonly encountered in the practice.

If a dentist has the consent of a patient to collect, use or disclose their health information, then the provider may use or disclose the information within the limits of that consent – subject to any specific use permitted under legislation (for example using information to assist in the location or identification of a missing person).

In addition, information may be used for a purpose (the secondary purpose) that is related to the primary purpose for which the information was given without obtaining express consent from the patient – providing the patient would reasonably expect the information to be used for the secondary purpose and the secondary purpose is related to the primary purpose.

For example, a reasonable secondary purpose may be disclosing the patient's information to an external pathology provider in order to obtain pathology results. The patient may not have specifically consented to their information being used for this purpose, but it is a secondary purpose related to the primary purpose (providing health care) and a patient would reasonably expect their information to be used to obtain the results.

15. What are the options if the patient lacks capacity to give their consent?

When consent is required, and a patient lacks capacity, a dentist may need to consider who can act on the patient's behalf. There may be a range of options, including:

- *a guardian;*
- *someone with an enduring power of attorney that can be used in relation to the patient's health;*
- *a person recognised by other relevant laws;*
- *a person who has been nominated in writing by the patient while they were capable of giving consent.*

As discussed in question 10, the Australian Privacy Commissioner considers that the collection of health information about third parties without their consent is permissible if the collection of that information is necessary to provide health services to a particular patient.

NOTE - The giving of consent for dental treatment is not covered in this manual and separate advice on this topic should be sought if required. See also the Dental Board of Australia Code of Conduct – section 3.5.

16. Can we disclose personal information to the media or in our direct marketing?

Ordinarily, the disclosure of personal information to the media by a dentist is not permitted without consent.

Any proposed use of patient information in the media, where that patient could be identified, must be raised and explained to the patient in detail. Consideration must also be given to whether the patient can be identified from a description of their treatment or appearance.

In any event, the patient should be given a copy of the proposed material to review prior to its use. If, after reviewing the proposed material, the patient consents to the use, their written consent should be obtained.

In one illustrative example dealt with by the Australian Privacy Commissioner, a health service provider made some comments to a newspaper about their work in a remote community. A case study was referred to, and although no identifying information was provided to the newspaper, the patient in question argued that the disclosure was sufficient to identify him within the community. The health service agreed and paid the patient financial compensation. (K v Health Service Provider [2008] PrivCmrA 11).

There are strict controls on the advertising of dental practices across Australia and the use of testimonials (including before and after photos) in advertising is prohibited. Penalties may apply and complaints may be made to the Dental Board of Australia.

17. In serious threats to life, health or safety can we disclose information?

Yes. The APPs and the HPPs contemplate the giving of information in this situation.

Victorian practices must comply with the HPPs which allow use or disclosure without consent if the practice reasonably believes that the use or disclosure is necessary to lessen or prevent:

1. *a serious and imminent threat to an individual's life, health, safety or welfare; or*

2. *a serious threat to public health, public safety or public welfare.*

For Tasmanian practices, use and disclosure is permitted under APP 6.2(c) which allows disclosure of information without consent if the APP entity:

1. *reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety; and*

2. *it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure.*

The Charter contemplates disclosure that is authorised by law (such as under APP 6.2(c)) and where disclosure is in the public interest.

Practitioners should note that there is a slightly different test that applies in Victoria and Tasmania, in that for Victorian practices, there is a requirement that there be a serious and ***imminent*** *threat. The threat need only be serious in Tasmania. Conversely Tasmanian practitioners must consider if obtaining consent is unreasonable or impractical. Victorian practitioners do not need to undertake such an assessment.*

Practitioners should also note that use or disclosure of information under the HPPs and APP is generally permitted for the purposes of assisting in locating a missing person providing the use or disclosure is not contrary to an express wish of the missing person.

The OIAC has released the Privacy (Persons Reported as Missing) Rules 2014 which set out considerations applicable to the giving of such information. HPP 2.5 is applicable for Victorian practitioners and also contains a number of specific considerations that must be taken into account before information is used or disclosed.

18. What if a health fund auditor/investigator or an Australian Dental Board representative asks us to supply copies of records for certain patients or to bring the records with us to an interview/informal inquiry?

Most health funds have as part of their contractual arrangements with a contributor (the patient) a clause that allows the health fund to access the patient's records for these purposes. If in doubt, ask the fund for the appropriate clause in their contract, or seek direct permission from the patient if you are not satisfied.

The HPPs and the APPs allow use or disclosure if that use or disclosure is required or authorised by law (for example in response to a subpoena or investigation under the National Health Practitioner Regulation Law).

19. If computerised dental records also contain details of failed appointments and/or bad debts, can these be released to other practitioners if the patient requests a transfer of their file?

All information collected in the course of providing a health service (such as appointment or payment history) is "health information" for the purpose of the Privacy

Act and the Health Records Act, and it must be treated as would any other health information.

Where a patient requests that a copy of their record be sent to another practitioner, details of payment information contained in the record could also be sent.

The manner in which this information is recorded should be taken into account at the time of entry, using only non-emotive, factual information, and if discussions with the patient are recorded, agreed outcomes should also be noted. Descriptions of personal attributes of the patient should be avoided.

20. Can patients' addresses be used to distribute practice newsletters?

Patient consent should be obtained before personal information is used to distribute digital or printed practice newsletters.

In addition however, APP7 requires dental practices to have a simple means by which the patient may easily request not to receive direct marketing communications from the practice. That is, although patient consent must be obtained, there must also be a simple process whereby the patient can withdraw their consent.

If newsletters are to be sent electronically, practitioners should also consider the operation of the federal Spam Act 2003 as there are significant penalties for sending unsolicited commercial material, such as newsletters. Documented patient consent is important in avoiding spam claims.

Part 4 – Data Quality matters (HPP3 / APP10)

21. How regularly are we required to seek and update information on a patient's medical history?

Under the APPs, organisations such as dental practices must take reasonable steps to ensure personal and health information they collect is accurate, up-to-date and complete. This requirement is also reinforced in the Dental Board of Australia Code of Conduct and Dental Records Guidelines.

In addition, dentists and dental practices must take reasonable steps to ensure that personal and health information used or disclosed is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2).

What is reasonable in the circumstances requires a consideration of the following:

1. *The type of health information they hold and how it is going to be used or disclosed;*

2. *Whether the information was collected directly from the individual or from a third party;*

3. *Whether certain "trigger points" provide an appropriate opportunity to recheck the accuracy of information (for example checking a patient's address each time they attend for an appointment);*

4. *The age of the information and whether it is to be relied upon in treating the patient;*

5. *Whether it would compromise patient care or safety if attempts were made to verify accuracy of the information; and*

6. *The extent of any adverse outcomes that may result from inaccurate, incomplete or out-of-date information being used by the practice.*

Importantly, a practice will not be excused from taking steps to improve data quality because of inconvenience or commercial cost.

The practice privacy policy must set out the means by which a patient can access information stored about them and how they may seek to have that information corrected.

Practitioners must always be mindful that inaccurate information about a patient may result in an adverse outcome. It is recommended that practices have systems in place to ensure changes to a patient's health status and medications are updated each time the patient attends. Practices should also ensure that a patient's contact details are current each time they present.

The following examples of reasonable steps that a practice may take are set out in the APP Guidelines for Chapter 10:

1. *implementing internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems)*

2. *implementing protocols that ensure personal information is collected and recorded in a consistent format*

3. *ensuring updated or new personal information is promptly added to relevant existing records*

4. *providing individuals with a simple means to review and update their information on an on-going basis, for example through an online portal*

5. *reminding individuals to update their personal information each time the APP entity engages with the individual*

6. *contacting the individual to verify the quality of personal information when it is used or disclosed, particularly if there has been a lengthy period since collection. (However, this step may not be reasonable where the APP entity has already taken other steps to ensure data quality, such as those outlined in the above list)*

7. *checking that a third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems. Depending on the circumstances, this could include:*

    a. *making enforceable contractual arrangements to ensure that the third party implements appropriate data quality measures in relation to the personal information the entity collects from the third party*

    b. *undertaking due diligence in relation to the third party's data quality practices prior to the collection.*

8. *if information is to be used or disclosed for a new purpose that is not the primary purpose of collection, assessing the quality of the data having regard to that new purpose before the use or disclosure.*

Part 5 – Data Security (HPP4 / APP11)

22. What strategies could be put in place?

Dental practices must take reasonable steps to ensure health information is securely stored. Any security strategy should include steps to protect against accidental loss and intentional security breach.

When deciding how best to protect a person's health information, dentists should consider:

- *Who should be allowed to see a patient's health records, records kept in a practice, or computerised records in a practice?*
- *When and how is it appropriate for one health service, such as a dental practice, to transfer information to another (for example, standard post may not be adequate for the sending of original records, where there is risk the information may be permanently lost)?*
- *What safeguards must apply when information is used for health research?*
- *Is the patient's consent needed for handling health information in each situation?*
- *How is health information destroyed when it is no longer needed? Is it securely shredded onsite or is it disposed of off-site?*
- *Are there computer system safeguards, such as password protection in place?*
- *Are paper records securely stored?*
- *Are there systems in place to ensure information is transferred securely (for example, not transmitting health information via non-secure e-mail)?*
- *Is there a system of monitoring the practice information system to test and evaluate data security?*
- *Are appropriate network security measures in place such as firewalls and anti-virus software?*

A key component of any data security system is staff awareness and training.

Staff must be made aware of the importance of privacy and the need to keep all records confidential – even if a patient no longer attends a practice.

Staff must be aware that misuse of health information (including a patient's contact details) can result in claims for compensation and may represent a breach of the Privacy Act in which case, fines and a gaol term may be imposed.

There must be clear protocols in place regarding secure destruction of old records to ensure compliance with the HPPs and accepted best practice. The practice's insurer may be able to provide guidance on the recommended length of time records should be kept.

Staff must also be made aware of security issues regarding access to a patient's Personally Controlled Electronic Health Record (PCEHR) and the Individual Healthcare

Identifiers. The PCEHR system must only be accessed by those individuals with appropriate practice authorisation. Penalties apply for unauthorised use of the PCEHR.

23. What if we lose a patient's record or there is a security breach?

APP 11 requires organisations to take such steps as are reasonable in the circumstances to protect information:

- *from misuse, interference and loss; and*
- *from unauthorised access, modification or disclosure*

*The key is that **reasonable** steps must be taken.*

The Office of the Australian Information Commissioner (OAIC) recommends that in the event of an information security breach (including loss of a patient record), four key steps must be followed:

Step 1: Contain the breach and do a preliminary assessment

Step 2: Evaluate the risks associated with the breach

Step 3: Notification

Step 4: Prevent future breaches

Practices must take each loss of a patient record (or any other security breach) seriously and move immediately to contain and assess the suspected breach - breaches that may initially seem immaterial may be significant when their full implications are assessed.

*Practices should undertake steps 1, 2 and 3 either simultaneously or in quick succession. In some cases it may be appropriate to notify patients immediately, that is before containment or assessment of the breach occurs. However, notification of patients is **not** required in all situations and consideration must be given to the effect of the loss or security breach and whether there is likely to be any harm to the patient.*

While notification is an important harm mitigation strategy, it will not always be an appropriate response to the loss of a patient's file or a security breach. The OAIC takes the view that providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notices of information security breaches. On this basis, each incident must be considered on a case-by-case basis to determine whether breach notification is required.

Ultimately however, the decision on how to respond to a security breach depends on the circumstance and, depending on the breach, not all the above steps may be necessary, or some steps may be combined. In some cases, practices may choose to take additional steps that are specific to the nature of the breach.

In relation to lost files practices should conduct an immediate investigation to determine:

1. *Whether the record been lost or misplaced;*
2. *Whether the record has simply been misfiled; or*

3. *Whether the record could have been inadvertently discarded in general rubbish.*

All reasonable attempts should be made to locate the record (including a search of rubbish if appropriate). If it cannot be located, detailed notes should be made regarding the circumstances of the loss and the attempts to locate. If necessary/appropriate, a new file should be created with the relevant notes. Attempts should be made to reconstruct the notes if that is possible from external sources.

The practice should also ensure that any deficiencies identified in practice systems are addressed to ensure the loss does not occur in relation to other patient files.

Once the practice has undertaken an investigation, the patient should be notified if appropriate in the circumstances. Consideration should also be given to notifying the Health Services Commissioner, Health Complaints Commissioner or Privacy Commissioner for guidance.

The OAIC has published a "Data Breach Notification" guide on the steps to be taken in the event of a privacy breach. This guide is available on the OAIC website.

Loss of electronic records is a particularly concerning matter as an entire practice can be affected by lost data which can include billing information, clinical notes and appointments.

A practice confronted with a loss of electronic data should engage experts to assist with the recovery process. A practice may also face a "ransomware" attack on its electronic data which prevents the data from being accessed unless certain demands (e.g. monetary or otherwise) are met. In cases of "ransonware" attack on electronic data, practices should notify the Police and engage an expert to assist with recovering the data.

Practices MUST have systems in place to ensure all data is regularly backed-up. Ideally a back-up should be kept off-site – although care should always be exercised if making arrangements for storage of patient information in the "cloud" as information may be stored off-shore.

Note that under APP 8.2, before using "cloud" providers located off-shore, practitioners must be satisfied that the provider is subject to legislation or a regulatory scheme that is substantially similar to the privacy protections set out in the APPs and there are mechanisms the individual can access to enforce the law or regulatory scheme in the foreign jurisdiction.

If a practice cannot be satisfied of these requirements, then consent of patients should be obtained before the patient's health information is transferred offshore – otherwise the practice will be liable for any breach of the APPs by the offshore storage provider.

24. What if our appointment book or computerised diary is visible from the other side of the reception desk?

You are required to take reasonable steps to prevent information about patients being made accessible to others. As in many similar circumstances, common sense must prevail.

25. What if we don't have locks on our file storage?

Patient files are required to be secure from view and interference by others. During the day, files should be away from patient traffic or waiting areas, or at least protected by a staff member in attendance in the vicinity at all times if the area cannot be sealed "off limits". At close of business, the dental practice and its contents is required to be secured from intruders. Again, common sense prevails.

26. What if our day list is posted on a whiteboard in the operatory?

In general, the posting of a day list on a whiteboard should be avoided.

If a "whiteboard" system cannot be avoided, find a location out of view of patients – e.g. inside the sterilisation room, on the back of the door. However consideration must also be given to who else may access areas of the practice where the whiteboard is positioned – for example, it would not be appropriate for sales representatives to see the day list for the entire practice.

27. What if a patient rings the practice asking for records to be transferred to another practitioner? What if another practice rings asking for records to be transferred on behalf of a patient?

It is advisable to seek a signed form of release from the patient directly, or as part of the request from the subsequent practitioner, have the patient co-sign the dentist's letter, giving his/her authority.

HPP11 provides that if a patient requests a transfer of their health information from one practice (the first practice) to another (the second practice), the first practice must provide a copy or written summary of that health information to the second practice. The first practice may charge a fee for the transfer providing the fee does not exceed the limits specified under the Health Records Act.

There are no equivalent Tasmanian provisions concerning the transfer of health information; however practitioners should follow the same processes as set out in HPP11 as following this process will ensure compliance with APP6.

Practitioners must always be careful to ensure that in transferring files or a summary of health information, that files are securely transferred and, as discussed above, that the recipient practice is expecting the files. Files should be sent directly to the recipient practice and not handed to the patient – particularly if there is information contained in the file that could cause harm to the patient or others, or if the files contain information given in confidence.

The transfer of files directly to the recipient practice is for the purpose of furthering a patient's care, which is different to providing the file to the patient who may use the file for different purposes. If patients require personal access to their health information, they may request to do so (in accordance with HPP6 and APP12), but the right to access is not absolute and may be refused in certain circumstances (see Question 33 below).

28. How should health information be transferred?

When transferring any health information, practices must take reasonable steps to ensure the health information is protected from unauthorized access or disclosure.

Dental practices should have systems and procedures in place to ensure health information is sent by an appropriately secure means. For example, higher security may be required when sending an original health record compared with sending a copy, given the loss of information would be permanent.

As a general rule, the general post is not appropriate for sending health records.

In one case for example, a patient complained to the Australian Privacy Commissioner when their health records and x-rays were mailed in the general post from one medical practice to another. Despite the fact that neither the records nor the x-rays were lost, and the recipient practice had been contacted to ensure the records had been received, the Commissioner formed the view that by using the general mail, the health service provider had failed to take reasonable steps to protect the complainant's personal information. (S v Health Service Provider [2008] PrivCmrA 19).

29. What if a person alleging they are from a health fund rings us to check what treatment we provided on a given date to a patient they say is a member of theirs?

Challenge the enquirer with some appropriate questions to check their bona fides, and if in doubt, ask for their supervisor's name and number and return the call.

Victorian practitioners should note that it is an offence under the Health Records Act to use false representation to gain access to health information and significant fines apply.

30. What if the security measures used by the dental practice to protect health information are breached?

In the event of a security breach, the steps and processes set out in question 23 should be followed.

Ultimately, proactive steps should be taken to ensure problems are rectified and that systems are put in place to ensure the breach does not occur in future. A practice that acts proactively is likely to be viewed in a favourable light if the matter is investigated by the Health Services Commission or the Office of the Australian Information Commissioner.

For example, the Australian Privacy Commissioner commenced an investigation of a medical centre after patient notes had been found scattered in a public car park adjacent to the medical centre. The medical centre had conducted its own investigation and had concluded that a lock on a medical waste bin kept outside at the rear of the centre had been tampered with. In response to the incident, the medical centre developed policies and procedures for the secure destruction of personal information and trained medical and administrative staff in the proper destruction of both medical waste and health records. The medical centre instructed its staff that health information was not to be left with general medical waste for collection. The medical centre also

obtained a shredder so that health records that were no longer needed could be securely destroyed on-site. The Commissioner was satisfied with the medical centre's response and no further action was taken. (Own Motion Investigation v Medical Centre [2009] PrivCmrA 6).

31. What if a patient requests that their health records be destroyed?

A patient's health records belong to the practice – they do not belong to the patient and the patient has no right to require that their health information be destroyed.

APP 11.2 provides that organisations (such as dental practices) must take reasonable steps to destroy or de-identify personal information, once it is no longer needed for any purpose for which it may be used or disclosed in accordance with the APPs:

- *if it is not contained in a Commonwealth record (which is not applicable to dental records); and*
- *if the organisation is not required by or under an Australian law (such as the HPPs), or a court/tribunal order, to retain the information (APP 11.2(d)).*

For Victorian Dentists, this means they must comply with the requirements of HPP4 in maintaining dental records in order to comply with the requirements of APP 11.2.

For Tasmanian dentists, there is no legislation specifying that records must be kept for a particular period of time. However, the standards set out in HPP4 represent good practice and accord with the retention periods recommended under the Guidelines published by the Dental Board of Australia and therefore, Tasmanian dentists should consider compliance with these retention periods.

In an example from NSW, the Australian Privacy Commissioner was asked to investigate a medical practice that had refused to delete a patient's health records after a request by the patient. The medical practice cited obligations under NSW legislation to maintain clinical records for 7 years. The Commissioner determined that because the medical practice had a legal requirement to maintain the record of the complainant's personal information for 7 years, reasonable steps required under NPP 4.2 (now APP 11.2) did not include the requirement to destroy or permanently de-identify the patient's personal information at the patient's request. (P v Private Health Service Provider [2008] PrivCmrA 16).

Practices must be aware that a patient's health records may be used by the practice to defend claims made by the patient.

Practices must also be aware that in Victoria, criminal penalties apply if documents are destroyed or rendered illegible and the documents were to be used or were likely to be used in evidence in a legal proceeding. Possible jail terms apply.

Dentists in both jurisdictions may also wish to seek advice from their insurer regarding optimum periods for retention of records from a risk management perspective.

Part 6 –Openness (APP1 / HPP5)

32. Is every practice required to have a privacy policy?

Yes. Every organisation under the terms of the legislation must have a clearly set out document that describes its policies on the management of personal and health information. The privacy policy must be kept up-to-date and at a minimum, it must include the following information:

1. *the kinds of personal information that the practice collects and holds;*
2. *how the practice collects and holds personal information;*
3. *the purposes for which the practice collects, holds, uses and discloses personal information;*
4. *how an individual may access personal information about the individual that is held by the practice and seek the correction of such information;*
5. *how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the practice, and how the practice will deal with such a complaint;*
6. *whether the practice is likely to disclose personal information to overseas recipients;*
7. *if the practice 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.*

The practice must take such steps as are reasonable in the circumstances to make its privacy policy available:

- *free of charge; and*
- *in such form as is appropriate.*

If a person or body requests a copy of the practice privacy policy in a particular form, the practice must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. (Note: APP 1.5 contemplates APP entities, such as dental practices making their privacy policies available on the entity's website).

Part 7 – Access and Correction (HPP6 / APP12 and APP13)

33. What is the patient's right of access?

Both the Privacy Act and the Health Records Act give individuals a right to access their health information.

Under both pieces of legislation however, the patient's right is not absolute, and access can be refused in some circumstances. For example, access can be refused if:

- *providing access would pose a serious threat to the life or health of any individual;*
- *providing access would have an unreasonable impact upon the privacy of other individuals;*
- *information has been given in confidence by a third party;*
- *the request is a repeated, unreasonable request for access to information that has already been provided;*
- *the request for access is frivolous or vexatious;*
- *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;*
- *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;*
- *providing access would be unlawful;*
- *denying access is required or authorised by or under law; or*
- *providing access would be likely to prejudice an investigation of possible unlawful activity.*

Patients also have a right to seek the correction of information held about them, if this is shown to be inaccurate, incomplete or not up-to-date. (See also question 21 on data quality).

Patients may request access to their health information in a variety of ways (subject to the circumstances in which access may be refused stated above). Access can be by way of:

- *inspection of health information, or if the health information is in electronic form, a print out of the health information that the patient can inspect and make notes of its contents; or*
- *the provision of a copy of the health information; or*
- *the provision of an accurate summary of the health information, instead of a copy, if the organisation and the individual agree a summary is appropriate; or*
- *inspecting the health information accompanied by an explanation of the information by a suitably qualified health service provider.*

34. Will a patient have to justify their request for access?

Patients do not have to give a reason when asking a dental practice for access to the health information a dental practice holds about them.

However, HPP6.1(k) and (l) provide that unreasonable repeated requests may be denied. APP12.3(c) provides that frivolous or vexatious requests can be denied.

35. Do requests to access health information have to be in writing?

Written requests for access are not required if the patient is seeking access to their own records.

However, under section 33 of the Health Records Act, requests for access by the patient's authorised representative or, if the patient is deceased, their legal representative, must be in writing. In addition, under the Health Records Act, if a Victorian Practice receives a verbal request for a patient's file (even if that request is made by the patient), the practice can ask that the request be put in writing. If such a request is made, the practice is not required to provide access until the written request is received.

There is no provision in the APPs that allow a health provider to request that a request for access be put in writing. However, guidelines released by the OAIC provide that if an APP entity (such as a dental practice) wants individuals to follow a particular procedure in making a request for access, the procedure should be published in the entity's privacy policy.

The reasons why a practice (both in Victoria and Tasmania) might want a request for access to be in writing include:

- *keeping track of requests;*
- *highlighting a pattern of requests; and*
- *maintaining a record of requests.*

Care should always be taken to ensure information is being given to the correct person. If there is any doubt, a practice should verify the identity of person making the request and if practical, seek confirmation of the request from the patient.

36. Is there any risk involved?

A risk in the access process is that a person may attempt to get access to another individual's information. Be wary and ensure this does not occur. See question 39.

If there is any concern that a request for access to a file, or for the provision of a copy of the file is not valid, the practice should undertake reasonable enquiries to contact the patient and verify the patient is aware of, and consents to, the request.

As discussed in question 29, practices should be aware that it is an offence under the Health Records Act to use false representation to gain access to health information and significant fines apply.

37. Can information be withheld?

Access to information can be withheld if the content of the record contains information that does not have to be given, or that the practice is prohibited from giving. (See question 33).

Written reasons (under the HPPs and APPs) must be given if access is refused or information is withheld.

38. What is a dental practice required to do when a patient asks for his or her health records to be corrected?

Patients have a right of correction under the APPs and HPPs and dental practices must take reasonable steps to correct the record to ensure it is accurate, complete and up-to-date.

If—

(a) the practice is not willing to correct the health information in accordance with an individual's request; and

(b) no other decision or recommendation has been made or is pending regarding correction of the information under the HPPs or the APPs or any other law; and

(c) the individual gives to the practice a written statement concerning the requested correction—

the practice must take reasonable steps to associate the statement with the information.

If the practice accepts the need to correct the health information but—

(a) the practice considers it likely that leaving incorrect information, even if corrected, could cause harm to the individual or result in inappropriate health services or care being provided; or

(b) the form in which the health information is held makes correction impossible; or

(c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so corrected—

the practice must place the incorrect information on a record which is not generally available to anyone involved in providing health services to the individual, and to which access is restricted, and take reasonable steps to ensure that only the corrected information is generally available to anyone who may provide health services to the individual.

If a practice corrects health information about an individual, it must—

(a) if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made; and

(b) take reasonable steps to notify any health service providers to whom the practice disclosed the health information before its correction and who may reasonably be expected to rely on that information in the future.

If an individual requests a practice to correct health information about the individual, the practice must take reasonable steps to notify the individual of a decision on the request as soon as practicable but in any case not later than 30 days after the request is received by the practice.

A request for correction should be completed within 30 days of receipt. A practice may choose to require written requests for correction and if so, that requirement should be stated in the practice privacy policy.

39. How should we process a request for access to information?

Practices must take reasonable steps to verify the identity of anyone seeking access to information before any information is provided.

There should also be checks in place to ensure the correct information is provided – for example there should be an alert system in place regarding similar patient names.

A recommended approach for handling an access request is to:

- *acknowledge the request and consider if the request should be put in writing (for example if the request is complex or specific information is sought);*
- *collate relevant information within the practice; and*
- *consider the form of access to be provided – has the person asked for a copy or have they asked for an explanation of their record. Consider if a summary of the information is appropriate and whether this form of access may be accepted by the applicant/patient;*

If the record contains information that may threaten the life or health of the individual seeking access, consider if an explanation of the record by a dentist (including an external dentist or colleague) is appropriate (see APP 12.5(b) and 12.6).

For Victorian practitioners, if a decision is made not to release information because of a threat to life or health, then the procedures set out in Division 3 of Part 5 of the Health Records Act must be followed. This includes providing notice to the patient that they can nominate a health service provider to assess the grounds for refusal to grant them access.

If a copy of the information is to be provided, ensure that information that is to be withheld is deleted or removed from the copy with an explanation as to why the information has been withheld;

- *confirm delivery arrangements with the patient/applicant;*
- *provide the information to the patient/applicant in the most appropriate and secure form.*

See also Part 13 below for information about charging fees for copying or other forms of access.

40. Does the practice have to provide information as sought by the patient?

The Australian Privacy Commissioner has taken the view that in general, access should be provided in the form requested by an individual, however, in some cases this may be neither possible nor appropriate.

In one illustrative example, a patient requested copies of their health records from their medical practitioner. The practitioner offered the patient the opportunity to view, but not copy, their health records. The patient was not satisfied with this offer. The Australian Privacy Commissioner concluded that although access should generally be granted in the form requested by the patient, an organisation is still able to meet the obligations imposed by NPP 6.1 by providing access in another form (now APP12 which provides that access may be granted in a way that meets the needs of the applicant and the practice). (A v Medical Practitioner [2009] PrivCmrA 1)

In another case however, a medical practitioner refused a patient's request for a copy of their health records on the basis that the patient did not have medical training and as such, providing a copy of the records could result in the patient misunderstanding their content. The medical practitioner had offered access to the records with assistance for interpretation however this was rejected by the patient. The Australian Privacy Commissioner disagreed with the practitioner's approach, finding that the practitioner's reasons were insufficient to justify refusal of the patient's request for a copy of the records. (B v Surgeon [2007] PrivCmrA 2).

Part 8 – Identifiers (HPP7 / APP9)

41. Can a practice use Medicare numbers to identify patients?

In general dental practices (and other health providers) cannot use an identifier assigned by a government agency or contracted service provider for the practice's own patient identification.

This means that Medicare numbers cannot be used by a practice to identify patients within the practice.

*However, it is possible for a dental practice to adopt a patients' unique Individual Healthcare Identifier (**IHI**) as the practice identifier, as this use is specifically authorised under the Federal Healthcare Identifiers Act 2010.*

Regardless of what identifier is used however, a practice must only use patient identifiers (such as numbers) if that use is reasonably necessary to enable the practice to carry out any of its functions (i.e. the delivery of care) efficiently.

Practices must ensure that their use of IHIs complies with the requirements of the Federal Healthcare Identifiers Act 2010 as misuse of IHIs may give rise to criminal penalties. In addition, misuse of IHIs is an interference with privacy and a breach of the Privacy Act. See question 7 above.

Part 9 – Anonymity (HPP8 / APP2)

42. Can a patient refuse to identify themselves when seeking treatment?

Under the HPPs and APPs, an individual must have the opportunity of not identifying themselves or of using a pseudonym when receiving health care – providing it is not impracticable or unlawful.

As a practical reality, it may be difficult to provide services on an anonymous basis – particularly if fees are to be collected from the individual, or it is necessary to establish Medicare eligibility.

It is not unusual however for patients to request that their records be stored under a different name and such requests should be complied with providing it is practical to do so.

If such a request is to be complied with, the practice must have secure means by which the practice can associate the real name of the patient with their pseudonym.

Part 10 – Transborder Data Flows (HPP9 / APP8)

43. What if a patient moves to the U.S.A. and his or her medical insurer requests records from you?

If the patient provides his or her consent, and this consent is both informed and current, then information about them can be transferred.

The consent signed by the patient must specify that if the patient consents to the disclosure of the information, the practice will not be required to take such steps as are reasonable in the circumstances to ensure the overseas recipient of the information does not breach the Australian Privacy Principles.

When providing the requested information, the original file should be retained by the practice and a record of the transfer should be kept in the file.

44. Is off-shore "cloud" storage permitted?

Off-shore "cloud" storage is permitted; however, under APP 8.1, it is the responsibility of the transferring entity (such as the dental practice) to take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the APPs.

The effect of APP 8.1 is that if the overseas recipient acts in a manner that is in breach of the APPs then, in certain circumstances, the act done, or a practice engaged in, by the overseas recipient is taken, under section 16C of the Privacy Act, to have been done, or engaged in, by the entity that transferred the data (the dental practice) and to be a breach of the APPs. In other words, the dental practice is liable for a breach by the overseas entity.

APP 8.2 provides that dental practices can avoid operation of APP 8.1 (and avoid liability for any possible privacy breach by the overseas "cloud" storage provider) if:

a. *the practice reasonably believes that:*

    i. *the recipient of the information (the "cloud" storage provider) 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 APPs 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.*

The OAIC has specified in its "Key Concepts" Guidelines, that a practice will have a "reasonable belief" if the practice applies a reasoned judgement to the circumstances at the time of making the relevant assessment.

If a practice cannot be satisfied that the requirements of APP 8.2(a) above can be met, then in general, consent of patients must be obtained before the patient's health information is transferred off-shore. That consent should comply with the requirements of APP 8.2(b).

Patient consent for transfer should be recorded.

As a prudent measure, you may wish to check whether your insurer is satisfied with mechanisms in place for the protection of patient information stored in the "cloud".

Part 11 – Sale, amalgamation, transfer or closure of a practice (HPP10)

45. What do I have to do if the practice is sold, transferred or is closed?

For Victorian practices, HPP 10 sets out in detail what is required if a dental practice is to be sold, transferred or closed. In addition the Victorian Health Services Commissioner has published a set of guidelines that add to the obligations set out in HPP 10.

In general, the sale, transfer or closure of a practice must be advertised in a local paper and at the practice location. Patients must also be contacted advising them of the sale, transfer or closure. In each case, the notification must include details of what is to be done with the health records held by the practice.

If a practice sale, amalgamation or closure is anticipated, dentists should familiarize themselves with the precise requirements of HPP10 and the relevant guidelines published by the Victorian Health Services Commissioner. The guidelines are available at: http://www.health.vic.gov.au/hsc/legislation.htm.

For Tasmanian dentists, there is no equivalent to HPP10 or the Health Services Commissioner Guidelines; however, Tasmanian practitioners should consider complying with these requirements as they represent best practice and will ensure practitioners comply with the Code of Conduct released by the Dental Board of Australia.

Part 12 – Transfer of records to another provider (HPP 11)

46. Can you share information with other dentists?

The multi-disciplinary team approach to health care sees practitioners work together and share necessary information, usually in accordance with codes of practice, to deliver optimum patient care.

Dentists involved in care and treatment for the ***primary purpose*** *and/or* ***directly related secondary purposes*** *would usually not need to seek further consent for necessary uses and disclosures. This will, however, depend on the circumstances of the case and the needs and wishes of the patient.*

For example, a patient may reasonably expect a dentist to discuss their case with colleagues within a practice for the purpose of providing that patient with appropriate care - in which case, it is unlikely that patient consent will be required before their information could be disclosed. On the other hand, it is less likely that a patient would expect external consultation about their case - and in these situations, patient consent should be sought before their information is disclosed.

In one case, a patient complained about disclosure of their health information between practitioners at a medical clinic. The patient had approached a consultant for treatment however the consultant had refused to treat the patient citing ethical and therapeutic reasons. The consultant then advised the clinic manager (who was also a medical practitioner) of the patient's need for treatment, the consultant's personal refusal to treat the complainant and the reasons for this refusal. Ultimately it was held that the disclosure of the patient's personal information to the clinic manager was both directly related to the purpose for which the information was collected, and was within the patient's reasonable expectations. (F v Medical Specialist [2009] PrivCmrA 8)

In general however, it is possible to discuss cases with colleagues and provide clinical details without a patient's consent if a patient cannot be identified from the information given. The same principle applies to presenting a case at a conference or in a peer reviewed journal.

At all times however, consideration should be given to whether the patient can be identified from their clinical presentation or clinical information – for example if a patient suffered a notorious injury that was the subject of a practitioner's discussions or publication.

47. Can we transfer records to another dentist on request?

If a patient wants to transfer their care to another dentist, they can request the disclosure of health information from the original provider to the new provider. A copy or a written summary of the record must be provided.

A practice that receives such a request should comply as soon as practicable.

Under the ADAVB Code of Ethics, transfer of records (without fee) ***to a colleague*** *to assist in the ongoing care of a patient is an ethical obligation of members.*

Part 13 – Administrative matters

48. What should we do if a patient makes a privacy complaint?

All complaints should be taken seriously and you should make every effort to ensure the complaint is resolved. The Privacy Act states that a complainant should take their complaint to the organisation before making a complaint to the OAIC. Dental practices must have in place a mechanism for dealing with complaints. You should consider the following questions:

- *Are individuals able to complain to your organisation?*
- *Does your organisation have an enquiries line or provide feedback or complaint forms in both printed and electronic formats?*
- *Is there a process by which privacy complaints are identified and directed to staff with appropriate knowledge of the Act?*
- *If an individual complains, are they being heard?*

49. Can we charge a patient for access to their health records?

Yes. The Health Records Act and the Privacy Act both permit patients to be charged for access to their records.

<u>Victorian practitioners</u>

For Victorian practitioners, the Health Records Regulations set a range of maximum fees that may be charged by holders of health information to recover the costs of providing people with access to their health information under the terms of the Health Records Act 2001.

The fees relate to three functions:

- *provision of access to health information to an individual;*
- *acting as a Nominated Dentist (Nominated Health Service Provider); and*
- *provision of health information to another dentist under HPP1.1.*

The stated objective of the fee setting regulation is to allow record holders to recover reasonable costs associated with the provision of health information, whilst ensuring the level of fees does not discourage individuals from exercising their right of access to health information. Dentists are not required to charge fees, and if they do, may charge lower fees than specified in the regulations. GST will apply to fees where appropriate.

The costs to be recovered by the charging of a fee relate to:

- *staff costs involved in locating and collating information;*
- *reproduction costs; and*
- *costs involved in having someone explain information to an individual.*

Part 5 of the Health Records Act provides the right of access in a number of different ways:

- *viewing the health information contained in the record, with or without the provision of an explanation of the information;*
- *provision of a copy of the health information, or a print-out of the health information contained in an electronic record;*
- *provision of an accurate summary of the health information; or*
- *inspection of the health information, with an opportunity to take notes.*

The table below shows fees specified in the Health Records Regulations 2012. Practices are advised to check the currency of fees at www.health.vic.gov.au/hsc

Table of Fees

See *http://health.vic.gov.au/healthrecords/regs.htm#tableoffees*

Item	Fee cap
Items 1 & 2 (Schedule 1): Time for supervising inspection or viewing of records	1.2 fee unit (currently equal to $15.00) per half hour or part thereof**
Use of equipment not in organisation's possession	Reasonable costs incurred
Item 3: (a)&(b) **Copy** of health information to individual	**20 cents per page** for A4 black & white Reasonable costs otherwise
(c) Time for **assessing & collating** health information	**2.5 fee units ($31.30)**
(d) Transporting records held off site	1.2 fee units ($15.00)
(e) Postage	Actual postage cost, if request to be posted
Item 4: Providing an **accurate summary** of information to individual	Greater of usual consultation fee (if a health service provider) or 2.9 fee units per quarter hour ($36.30), up to 9.4 fee units ($117.80)
Item 1 (Schedule 2) **Copy** of health information to **another health service provider**	20 cents per page for A4 black & white if at least 20 pages Reasonable costs otherwise
Item 2: **Summary** of health information to another health service provider	Greater of usual consultation fee or 2.9 fee unit per quarter hour ($36.30), up to 9.4 fee units ($117.80), where the time taken to prepare is at least 30 minutes
Regulation 7: Functions of nominated health service provider under s. 42 of the Act	Reasonable costs not exceeding 4.7 fee units per quarter hour ($58.90) up to 23.6 fee units ($295.70)

(The indicative fee amounts reflect that fee unit values are rounded to 1 decimal point, and that in calculating fee amounts, fees are rounded to the nearest 10 cents. The fee unit value of $12.53 applies to 2012-13 and has been used in the above calculations.*

*** The current fee for supervision is expressed in terms of quarter hours. However, in order to make use of the Monetary Units Act, the fee units must be expressed as 1 fee unit or more. Therefore this has changed to be expressed in terms of a half-hour, although the Regulations provide for charges to be made in quarter-hour increments.)*

Tasmanian practitioners

Tasmanian practitioners are not subject to the same level of specificity in the amounts that can be charged for a client to be given access to their records.

APP 12.8 provides that private entities such as dental practices may charge for giving an individual access to their information; however, the charge must not be excessive and must not apply to the making of the request.

50. Can a dental practice disclose personal health information it has collected to a third party such as a health fund, where the patient is a member of that fund?

The practice may use or disclose personal health information for a purpose (the secondary purpose), which is directly related to the primary purpose of collection, if this is within the reasonable expectation of the patient. Such secondary purposes may include the management, funding and monitoring of a health service, together with complaint-handling, planning, evaluation and accreditation activities. See also Question 18 above.

51. Can a dental practice report a patient's payment default to a credit reporting agency?

The Privacy Act allows a 'default listing' on the individual's consumer credit file if it relates to 'credit provided by a credit provider' and certain other conditions set out in the Act are met. The Australian Privacy Commissioner has taken the view that listing a payment default will be an interference with a patient's privacy if the health service provider is not a credit provider under the Act. Specific conditions must be met before a dental practice could be considered to be a 'credit provider' for the purpose of the Privacy Act.

In one case, a health service provider had reported a patient to a credit reporting agency for an outstanding bill. The health service provider argued that because the patient was given 7 days to settle their account, a credit arrangement existed between the health service provider and the patient, and as such, the health service provider was a 'credit provider'. This was rejected by the Australian Privacy Commissioner who found the patient's privacy had been breached. The health service provider apologised, removed the payment default, and ceased its practice of reporting overdue accounts to a credit reporting agency. The patient also accepted a confidential financial settlement. (L v Health Service Provider [2009] PrivCmrA 15).

Dentists should seek advice before deciding they are 'credit providers' with a power to report patients to credit reporting agencies.

52. Are there child/adult guidelines?

The Privacy Act does not set an age limit at which a child or young person can exercise their own privacy rights – this occurs when the individual becomes competent to make such decisions. Where a child or young person is competent they should make their own decisions; if they are not competent to do so, a dentist may discuss their health record with a parent.

If a parent seeks information about their child, but the child explicitly asks that certain health information not be disclosed to that parent, the dentist may consider it appropriate to keep such information confidential.

53. How are complaints to the Privacy Commissioner handled?

Complaints about alleged breaches of privacy can be made to the Australian Privacy Commissioner, and in Victoria, the Health Services Commissioner, and in Tasmania, the Health Complaints Commissioner. The Commissioners can investigate, conciliate and, if necessary, make determinations about complaints. Penalties may apply if a practice fails to cooperate with an investigation and in some situations compensation may be ordered. Penalties may also be imposed for repeated or serious breaches of the Privacy Act.

54. What are some other examples of how health services have been affected by privacy legislation?

The Australian Privacy Commissioner publishes case notes if the Commissioner considers there is some public interest in the publication. Some relevant cases have been referred to above. Additional cases can be accessed from the OAIC website at http://www.oaic.gov.au

FURTHER QUESTIONS

If you have any further questions regarding privacy or the privacy legislation, please contact the Branch on 8825 4600 or by email on ask@adavb.net

THE PRACTICE PRIVACY ACTION CHECKLIST

The Practice Audit Checklist at 4.1.5 can be used to identify practices, procedures and systems that need to be addressed as part of completing this Checklist.

Action	Start	Program	Completion	Follow up
• Review practices, procedures and systems to ensure compliance with the APPs				
• Privacy Policy in place that is clearly expressed and up-to-date and is freely available to patients (including availability on the practice website).				
• Privacy Officer appointed				
• Staff and patients informed and educated on privacy and its importance				
• Privacy audit conducted o Actions should include (but not be limited to): o Review access logs o Review and analyze any complaints o Check for any legislative or professional policy changes o Review security procedures o Check operation of data integrity measures (backup)				

• System in place for patients to request access to their information				
• Modify practice accounts to allow for access fees where appropriate (ensuring any access fees are not excessive or, for Victorian practices ensure the fees comply with the Health Records Act).				
• Implement procedures that enable patents to receive care anonymously or by using a pseudonym – clearly setting out where this may be possible and how it will be managed.				
• Review collection notice and procedure for making patients aware of the collection statement				
• Review procedures for dealing with unsolicited information about patients, including receipt of information given in confidence				
• Review direct marketing procedures to ensure compliance with professional and privacy obligations and ensure compliance with anti-spam legislation				
• Review arrangements regarding offshore transfer of patient data, including the use of overseas “cloud” storage providers to ensure compliance with the APPs.				
• Review procedures and policies for the use of government related identifiers				

including the use of Individual Healthcare Identifiers.				
• Review procedures used to ensure patient data is correct, up-to-date, accurate and relevant for the provision of dental care				
• Review record retention practices and procedures including review of document destruction processes to ensure compliance with privacy obligations				
• Review procedures for patients to correct their health information				
• Review complaints handling procedure				

Reviewed: ____ / _____ / ____ By Whom: _____

Checked: ____ / _____ / ____ By Whom: _____

THE PRACTICE PRIVACY POSITION

The Practice recognises and supports the right of all patients, staff, suppliers, contractors and members of the public to privacy and confidentiality of their private and personal records.

State and Federal privacy laws aim to protect the privacy of individuals, particularly where health information is concerned.

The Practice has produced a set of policies and procedures in accordance with the privacy legislation to ensure the privacy of individuals is protected at all times.

All employees, agents, suppliers (and if and where applicable members of the public), are required to adhere to the policies and procedures at all times.

To confirm the Practice's policies and procedures are appropriate and to ensure that all relevant parties are adhering to them, the Practice has created a Complaints and Incident Register.

All employees are required to be vigilant in ensuring that systems and procedures are maintained to ensure the policies are not breached. If an employee is aware of a breach or of a deficiency in the practice's procedures that may result in a privacy breach, they should record the matter in the Register (see also Sections 4.3.3 and 4.3.4).

All complaints received, no matter how minor they may appear to be, must be recorded in the Register. The senior dentist – or if not available – the next senior member of staff must be advised of each entry as it is recorded for review and action. The "Data breach notification — A guide to handling personal information security breaches" published by the Office of the Australian Information Commissioner will be used as the framework to handle complaints.

The Register will be used to gauge the number and nature of the complaints, and whether a particular issue is re-occurring. All staff must therefore be accurate in the recording of details of complaints.

Signed: _____

Name: _____

Position: _____

Date: _____ / _____ / _____

PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORD (PCEHR) SECURITY AND ACCESS POLICY

This sample policy has been developed from a NEHTA template policy. The policy should be adapted for use to ensure it meets the needs of individual practices.

PURPOSE

This practice participates in the national Personally Controlled Electronic Health Record (PCEHR).

All staff and contractors are expected to know that use of the PCEHR is highly regulated to ensure individual health records are not misused or inappropriately accessed. Penalties apply for misuse of the PCEHR and disciplinary act must also be taken against staff found to misuse or inappropriately access the PCEHR.

This policy is designed to provide guidance for staff and contractors about access to, and use of the PCEHR.

SCOPE OF POLICY

This policy applies to all employees and contractors working at the practice.

RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE MONITORING

In accordance with the *Healthcare Identifier Act 2010* (Cth), the practice has appointed individuals to the following positions:

1. Responsible Officer: The RO has legal responsibility for compliance with this policy and compliance with the eHealth System legislation.
2. Organisation Maintenance Officer: The OMO is responsible for implementation and compliance monitoring of this policy, and for maintenance of the policy.

RELATED DOCUMENTS/LINKS

This policy is to be read in conjunction with the following documents:

1. Personally Controlled Electronic Health Record Rules 2012
2. Personally Controlled Electronic Health Records Act 2012
3. Personally Controlled Electronic Health Records Regulation 2012
4. Healthcare Identifier Act 2010

AUTHORITY TO ACT

The RO and OMO for the practice are authorised to act on its behalf in dealing with the Department of Health and Ageing.

ACCESS FLAGS

The RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation.

In setting and maintaining access flags, the RO/Seed OMO will ensure that:

1. Consumers are able to determine and control access to their eHealth records in a way that meets reasonable public expectations. Network organisations that would not be expected by consumers to be connected will thus have their own access flags.
2. The organisation is able to share health information internally in an appropriate manner.

The RO/OMO will undertake reviews of the network structure and access flag assignments at such times as the structure changes, or in the case that a regulatory or consumer query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the Department of Health and Ageing.

MAINTAINING RECORDS OF PCEHR USE WITH THE DEPARTMENT

the RO/OMO will establish and maintain an up-to-date records required by the Department of Health and Ageing.

The OMO will also maintain an accurate and up-to-date list of individuals within the practice who are authorised to access the PCEHR system and, if an individual is no longer authorised to access the provider portal on behalf of the practice, the OMO will ensure the Department of Health and Ageing is informed and the individual removed from the list of authorised users.

ACCESS TO THE PCEHR

Practice staff and contractors must only access the PCEHR if access is required to undertake their duties.

All individuals who require access to the PCEHR will be provided with a unique user account with individual login name by the OMO.

The practice will maintain records of user accounts, and individuals given access to the PCEHR must not reveal their passwords to any other individual.

The RO/OMO will immediately suspend or deactivate individual user accounts in cases where a user:

1. leaves the organisation
2. has the security of their account compromised
3. has a change of duties so that they no longer require access to the PCEHR system.

User accounts will not be used by multiple staff members. All users will ensure that they log out of the system when they are not using it to prevent unauthorised access.

All staff and contractors are reminded that a failure to secure log-in details may result in misuse of the PCEHR being attributed to them and penalties may apply.

IDENTIFICATION OF STAFF MEMBERS WITH AUTHORISED ACCESS TO THE PCEHR SYSTEM

The OMO will maintain a record of authorised Healthcare Provider Identifier – Individual numbers in the clinical software and in the organisation's internal records. The clinical software will be used to assign and record unique internal staff member identification codes. This unique identification code will be recorded by the clinical software against any PCEHR system access.

The practice will maintain such records (for example staff rostering records) as to allow it to determine which user accessed the system on a particular day. These records must be maintained to allow audits to be conducted by the Department of Health and Ageing.

Where required, the practice will maintain staff rostering records to assist in identifying particular authorised users that have accessed the PCEHR system.

STAFF TRAINING
Staff and contractors who require access to the PCEHR must undergo PCEHR training prior to being authorised to access the PCEHR system on behalf of the practice.

Staff training will provide information about how to use the organisation's clinical software, and/or the PCEHR Provider Portal, in order to access the eHealth record system accurately and responsibly.

If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the PCEHR system.

The OMO will oversee a register of staff training as it relates to the PCEHR.

REPORTING SECURITY BREACHES
A security breach occurs when any unauthorised person accesses the PCEHR, or when a staff member with access to the PCEHR discovers that someone else may have gained access to their user account.

If any staff member or contractor becomes aware of a security breach, they must follow the reporting procedure outlined in the procedures section below. All breaches must be reported to the OMO/RO who will ensure that the breach is reported to the Department of Health and Ageing.

RESPONDING TO PATIENT COMPLAINTS
The practice will make patients aware of the process for raising issues or complaints and will keep a record of complaints, and the patient will be made aware of the ability to lodge a complaint with the Office of the Australian Information Commissioner.

MAINTAINING THE PCEHR POLICY
The OMO is responsible for ensuring the accuracy of the organisation's PCEHR policy and its compliance with PCEHR legislation. The OMO will ensure that the policy remains current and reflects changes in PCEHR legislation and in the structure of the organisation.

REPORTING SECURITY BREACHES
If any staff member becomes aware that their user account has become compromised or that someone has used their computer to gain unauthorised access to the PCEHR, they are to immediately inform the RO/OMO. If only the OMO is informed, it is the OMO's responsibility to ensure that the RO is made aware of the issue.
The RO/OMO will create a log entry of the breach including details of the date and time of the breach, the user account that was involved in the unauthorised access, and which patient's information was accessed (where known).

The RO/OMO will also undertake appropriate mitigation strategies, including, but not limited to:
1. Suspending/deactivating the user account;
2. Changing the password information for the account; and
3. Reporting the breach to the System Operator.

MAINTAINING ORGANISATION'S PCEHR POLICY

The OMO must maintain this policy and ensure the policy is reviewed at least annually.

The OMO will ensure that copies are kept of each version of the PCEHR policy and that new versions of the policy are easily identifiable.

PCEHR POLICY CHECKLIST

- ☐ Responsible Officer and Organisation Maintenance Officer roles assigned to people with appropriate levels of authority and legal responsibility
- ☐ Network hierarchy and access flags set in a way that meets reasonable consumer expectations (where appropriate to size and structure of organisation)
- ☐ Individual Clinical Information Software (CIS) logins and secure passwords assigned to all staff with access to the PCEHR
- ☐ Internal record of authorised users with PCEHR access retained including individual clinical software identification codes.
- ☐ Policies and procedures in place to govern access to the PCEHR
- ☐ Staff provided with PCEHR training and given ongoing access to PCEHR policy
- ☐ Where provider portal access is authorised for staff, an up-to-date list of authorised healthcare providers maintained
- ☐ Systems are in place to ensure that on request, patients are provided with information about complaints procedures.

THE PRACTICE PRIVACY POLICY

Our practice reviews and updates this Privacy Policy on a regular basis.
Our privacy officer is – identify officer and contact details such as phone number and email address.

Delete this text after customising:

This document contains a privacy policy that is intended to meet the requirements of the Privacy Act 1988. The policy can be adapted to the needs of individual practices by altering the blue text (i.e. change font to black, amend or delete). However, all privacy policies must contain certain information so we recommend that you do not change any of the black text. Ensure the Privacy Policy is easily available to patients, including placement on the practice website.

Our practice respects your privacy

We take your privacy seriously.

We are bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988* (**Privacy Act**) and *the Health Records Act Victoria 2001.*

[Insert for Tasmanian practice … *The practice is also bound by the Tasmanian Charter of Health Rights and Responsibilities*.]

Our Privacy policy outlines how we use and manage your health information. A Notice to Patients is posted in our patient waiting area as a summary statement of the policy.

Collection and use of information

We collect health information directly from you and your authorised representatives to provide you with dental treatment.

Personal information such as your name, address, health insurance and financial details are used for the purpose of addressing accounts to you, as well as for processing payments, collecting unpaid invoices via an external collection agency, and writing to you about our services and any issues affecting your health care.
As this practice is undertaking accreditation, some of your details may be released to the accrediting agency. The accreditation agency is also bound by the privacy act. We may de-identify and use your information and data for research, evaluation and benchmarking purposes.

We may also collect health information from a third party such as a health fund or referrer.

We will only collect your e-mail address if you send us a message or you provide us with your address directly. It will only be used for the purpose for which you

provided it. You have the option of having your email address deleted from our records at any time.

Non-disclosure of information

If you choose not to provide us with information relevant to your care, we may not be able to provide a service to you, or the service we are asked to provide may not be appropriate for your needs.

Importantly, you could suffer some harm or other adverse outcome if you do not provide information relevant to your care.

Website Security

Our Internet Service Provider {insert name of ISP here} makes a record of your visit to our practice website and logs the following information for our reference:

- Your server address
- Your domain or top level domain name (for example practice.com, .gov, .au, etc.)
- The date, time and duration of your visit to the site
- The pages you accessed and documents downloaded
- The previous site you visited
- The type of browser you are using
- Your ISP may collect more or less information for you

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

Our website contains links to other websites. We are not responsible for other websites' privacy practices, and care should be taken when providing personal information on any website.

Cookies

This website only uses session cookies during a search query of the web site.
Upon closing your browser the session cookie set by this website is destroyed and no personal information is maintained.

Employer/employee responsibilities

All staff employed in this practice are required to undergo training to understand their responsibilities in maintaining your privacy and to sign a confidentiality agreement in order to protect your personal information.

Disclosure

The purpose of collecting your information is to provide you with a dental service; for internal and external administrative purposes, insurance purposes and record keeping.

We will not use your health information for any other purpose unless one of the following applies:

1. You have consented;
2. You would reasonably expect that your information may be used for that purpose; for example we may disclose your health information to another health service provider such as a specialist dentist, a technician, your GP or another health practitioner for the purpose of providing you with health care; or
3. The use of your health information is required or authorised by law.

Data quality

The practice takes steps to ensure that the health information we collect is accurate, up to date and complete. These steps include maintaining and updating personal and health information when you attend the practice or you advise us that your personal information has changed.

Data security

The practice keeps hard-copy, electronic records or a hybrid of both.

We protect them by ensuring hard-copy records are kept in locked files and there are security processes in place regarding computer access. Electronic data is backed-up.

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

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

If there are specific security measures in place use this clause:

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

- insert details of the security measures that you have adopted/deployed, such as encryption, password protection, secure sockets etc.

Access and correction

You can request access to your health or personal information we hold, or request that we change that information.

Requests for access or correction must be in writing and directed to the practice Privacy Officer.

You can access or make changes to your health or personal information unless we consider that there is a sound reason under the Privacy Act, or other relevant law to withhold the information, or not make the changes.

The practice may charge for access to or copies of health records.

After a period of 7 years (and if you attended the practice as a child, you have reached the age of 25) we may destroy your records in accordance with applicable laws.

Marketing

Our practice may use your information for the purpose of direct marketing; however, we will not on-sell your personal information.

We understand that you may not wish to receive marketing materials. If you would prefer not to receive such information, please approach the Privacy Officer or another staff member at the practice

Sending information overseas

As part of maintaining your records, the practice may use off-site electronic data storage providers, transcription service providers, professional indemnity insurers, marketing agencies or other third party service entities. These providers may be located offshore.

We will try to inform you about where your information is sent. Please be assured that we take reasonable steps to ensure compliance with the Australian Privacy Principles in relation to any off-shore transfer of your information.

Complaints

If you suspect there has been or may have been a breach of your privacy, you can complain directly to the practice Privacy Officer. (See Enquiries below).

We take complaints very seriously.

You can lodge a complaint in a number of ways: by phone, email, in writing or in person.

Your complaint will be reviewed in house.

Any appropriate corrective action required to manage this breach and any preventive actions required in order to prevent breach in future will be discussed and decided.

You will be sent a letter explaining the review process and the consequences of the review.

In the event of a privacy breach, we will comply with applicable guidelines issued by the Office of the Australian Information Commissioner.

For more information about Privacy laws, or to raise concerns about any matter not satisfactorily resolved with the practice you can contact the Office of the Australian Information Commissioner (www.oaic.gov.au or ph. 1300 363 992).

[Insert for Victorian practices … Privacy and general complaints about your care can also be directed to the Health Services Commissioner.
Insert for Tasmanian practices … Privacy and general complaints about your care can also be directed to the Health Complaints Commissioner.]

Enquiries

For further information about the practice's management of privacy, please contact our Privacy Officer **[insert contact details].**

DOCUMENT DETAILS	FOR OFFICE USE ONLY (NOT FOR PATIENT)
This policy should be reviewed annually and any changes to policy and actions required should be documented and signed.	
Responsible person:	**[Insert the name or title of the person responsible for reviewing this document]**
Review cycle:	**[Insert your practice's review cycle]**
Date of last review:	**DD/MM/YYYY**
Action required:	
Signed:	

NOTICE FOR PATIENT

Your Privacy

Delete this text after customising:

This Notice to Patients is a summary of the Practice Privacy Policy and outlines to patients how and why we collect information about them. This notice should be customised and displayed in a prominent place in Waiting Room or at Reception. This is not a complete privacy policy.

We respect your right to privacy and we have systems in place to ensure we comply with the Australian Privacy Principles. This statement is a brief summary of our practice's privacy policy. Our complete policy is available on request.

Our practice [**insert name of practice and ABN**] trading as [**insert trading name of practice**] collects health information about you in order to provide you with dental services. Personal information collected such as your name, address, contact details, health insurance and financial details are also used to address accounts to you, process payments, collect unpaid invoices via an external collection agency and to contact you about our services and any issues affecting your health care.

We may collect your health information from other health care professionals, or disclose it to them if, in our judgement, it is necessary in the context of your care.

If you choose not to provide us with information relevant to your care, we may not be able to provide a service to you, or the service we are asked to provide may not be appropriate for your needs. Importantly, you could suffer some harm or other adverse outcome if you do not provide us with relevant information.

We will securely store your records, such as x-rays, treatment and personal details, and any other material relevant to your care. Our complete privacy policy sets out how you can access or seek correction of your records.

Our privacy policy details how you can lodge a privacy complaint and how we will deal with such a complaint.

For administration purposes, we may rely on service providers located outside Australia. We will take reasonable steps to ensure that any offshore data transfer complies with Australian privacy laws. Whilst our practice takes all reasonable steps to ensure security of your information, we cannot guarantee secure transmission of information over the internet.

Our practice Privacy Officer can be contacted at the practice during business hours if you have any concerns or questions about a privacy matter [insert contact details].

PRACTICE COMMITMENT TO PRIVACY LEGISLATION

Protecting your privacy and personal information has a high priority in the way this practice is conducted.

This practice's policies are designed to comply with all state and national legislation, in particular the Australian Privacy Principles (**APP**).

[insert for Tasmanian practices] The practice is also committed to upholding the rights of patients under the Charter of Health Rights and Responsibilities.

This practice commits to:

- only collecting information about you in accordance with the APPs;
- being fair and open in the way we collect the information, and only collecting information actually required in the course of providing you with health care;
- retaining your information in a secure environment and will only provide essential information to our agents or service providers for the purpose of conducting our practice with you;
- binding all staff, agents and service providers to our confidentiality agreements and our Privacy Policies;
- not sharing or selling your information to any third party for marketing purposes and not releasing information unless required by law to do so;
- allowing you access to the personal information held about you and inviting you to advise us if you think any information is incomplete, inaccurate or out-of-date;
- where possible, satisfying your requirements by amending any information that you may consider incomplete, inaccurate or out-of-date;
- if you require, allowing you to deal with the practice anonymously wherever practical;
- providing you with a copy of our Privacy Policy if you require it;
- explaining the reasons for collecting information, how we use it and the consequences of not having the information required.

For further information you can contact the practice in person, by phone or email and we will be happy to respond to your enquiry.

THE PRACTICE AUDIT CHECKLIST

This Practice Audit Checklist can be used to identify practices, procedures and systems that need to be addressed as part of completing the Practice Privacy Action Checklist at 4.1.1.

Question	Response	Further action required	By whom?	By when?
• What personal information does the practice collect?				
• How does the practice collect health information? Include: standard forms? customer surveys? loyalty programs? or online interaction?				
• Where and how does the practice store this information? In a single database? In a number of sites?				
• Who within the practice has access to the health information it holds?				
• Who actually needs to have access to the information?				
• Has the practice taken such steps that are reasonable in the circumstances to ensure health information is protected from misuse, interference and loss, and from unauthorised access, modification or disclosure?.				

• Are all staff aware of the practice's privacy policies and procedures?				
• Why does the practice collect the personal and health information it collects?				
• Does the practice need the information it collects for the purposes for which it was collected?				

Question	Response	Further action required	By whom?	By when?
• Would individuals know the practice is collecting the information?				
• Are there systems in place to deal with unsolicited information and information given in confidence?				
• How does the practice use the information?				
• Does the practice give the information to anyone outside the practice?				
• Does the practice contract out any functions or activities involving personal or health information?				
• Does the practice take any privacy measures to protect this information?				
• Does the practice make individuals aware of the practice's intended uses and disclosures of that information?				
• Is relevant personal and health information accurate, complete and up to date?				

• Does the practice transfer information overseas for example to a cloud storage provider?				
• When providing their personal information, can patients choose whether their information will be used for marketing purposes?				
• Is there a simple process that allows individuals to request that they are not sent marketing information?				

• In relation to marketing using client's email addresses are there systems and process in place to ensure that messages:
  • are only sent with the addressee's consent - either express or inferred consent;
  • are sent without revealing the email addresses of other recipients;
  • include clear and accurate information about the person or business that is responsible for sending the message; and
  • have a functional unsubscribe facility.				

• Are there processes in place to ensure that any unsubscribe requests in relation to electronic marketing material is acted upon promptly?				

• Have there been any significant changes in legislative privacy obligations since the last audit?				
• Is the practice privacy policy freely available to patients, such as on the practice's website?				
• Is the practice Privacy Officer familiar with the APPs?				
• Are there clear processes in place that allow patients to request access or alteration of their records?				
• Are fees for access in line with statutory requirements?				
• Is the practice collection statement up-to-date?				
• Are there systems that allow (if possible) patients to deal with the practice anonymously?				
• If the practice uses the Personally Controlled Electronic Health Record system, are there procedures in place to ensure the practice complies with its obligations relating to use of the system?				
• If the practice uses Individual Healthcare Identifiers (IHI), are there systems in place to ensure the IHIs are not misused?				
• If offshore storage of health information is used, does the practice comply with APP 8.1 and 8.2.				

• Are there procedures in place regarding destruction of records that comply with applicable laws?				
• Are there complaints procedures in place that allow individuals to easily make complaints about privacy breaches?				

Signed: _____

Date: _____ / _____ / _____

THE PRACTICE RECORD CHECKLIST

This practice considers the following questions in terms of each record:

Question	Comment	Further Action Y / N	Action	By Whom	Date Complete
• What is the primary reason for the existence of the record?					
• Who or what is the source of the information?					
• Has the individual's consent been obtained concerning the record's collection, management and uses of the information?					
• How is the information collected?					
• How is the record kept up to date?					
• Where is the record stored?					
• How is it stored?					
• Who has access?					
• What is the process for access?					
• What is it used for?					

Reviewed: ____ / _____ / ____ By Whom: _____

Checked: ____ / _____ / ____ By Whom: _____

THE PRACTICE PRIVACY PROGRAM

The following is the information collected and retained by the practice.

The reasons for collecting the information, the staff that have access to the information and the purposes for which they may access the information is detailed.

Details	Reason for Collecting	How Long Information is Retained	Who has Access?	Reason for Access
Patient Medical History				
New Patient Information				
Patient Case History Record				
Re-examination/History Form				

Reviewed: ____ / _____ / ____ By Whom:
_____

Checked: ____ / _____ / ____ By Whom:
_____

WEBSITE PRIVACY & POLICY STATEMENT

contains an example of a Website Privacy

What must the website privacy statement tell a site visitor?

1. That the practice has developed a policy to protect patient privacy in compliance with privacy legislation;
2. What personal information is being collected;
3. Who is collecting their personal information;
4. How their personal information is being used;
5. To whom their personal information is being disclosed; and
6. How their personal information is being stored.

The practice privacy policy (see 4.1.3) should be made available on the practice website with the additional information included from below.

{You may need to collect certain information and/or assurances from your Internet service provider in order to complete this statement – see Section 4.4.1 for this}

Web Site Privacy Policy

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

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

Information Collected

When you look at this web site, our Internet Service Provider ***{insert name of ISP here}*** makes a record of your visit and logs the following information for statistical purposes:

- Your server address
- Your domain or top level domain name (for example practice.com, .gov, .au, etc)
- The date and time of your visit to the site
- The pages you accessed and documents downloaded
- The previous site you visited
- The type of browser you are using
- ***{your ISP may collect more or less information for you}***

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

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

Access to information collected

We will not make an attempt to identify users or their browsing activities. However, in the unlikely event of an investigation, a law enforcement agency or other government agency may

exercise its legal authority to inspect our Internet Service Provider's logs, and thus gain information about users and their activities.

Use of information collected

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

Personal health Information

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

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

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

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

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

Cookies

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

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

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

SALE / TRANSFER / CLOSURE OF DENTAL PRACTICE

The following text may be edited for use as a notice to be posted at the entrance to the practice or for publication in a local newspaper. Practitioners in Victoria and Tasmania should consult HPP 10 of the Victorian Health Records Act and associated guidelines for direction on notice requirements. (See also Section 4.2.8 – Letter to Patients and Section 3)

(insert name of principal or executor)

Dr …… wishes to announce the sale / transfer / closure of his/her dental practice located at ……[**insert address**]……..

If sold/transferred

The practice has been sold / transferred to Dr …….. [**or alternative business name**] effective from ….[**insert date**]….., and he / she / they will be pleased to continue providing dental care to the practice's patients. The previous owner has retired / relocated and extends appreciation to all patients who attended for treatment over the years.

Patient records

Dental records held by the practice will be: [**insert whichever is appropriate**]

- transferred to Dr.....[**insert name or alternative business name**].....on [**insert date at least 21 days after notice published**]; or
- retained in the possession of Dr [**insert name of original dentist**].

Patients wishing to have their dental record transferred to another dentist or practice should contact [**insert name of contact**].

If closed

The practice has been closed due to the retirement / ill health / death of the principal …(insert name…). Previous patients of the practice may wish to seek their dental care from …… (or another local practice).

Patient records

Dental records held by the practice will be: [**insert whichever is appropriate**]

- transferred to Dr.....[**insert name or alternative business name**].....on [**insert date at least 21 days after notice published**]; or
- retained in the possession of Dr [**insert name of original dentist or alternative name**].

Patients wishing to have their dental record transferred to another dentist or practice should contact [**insert name of contact**].

PATIENT RECORD DISCLOSURE – LOG SHEET

PATIENT NAME	RECORDS TRANSFERRED OR DISCLOSED TO		DATE OF TRANSFER / DISCLOSURE	NOTES (EG. RE NATURE OF RECORDS AND CIRCUMSTANCES REQUIRING DISCLOSURE)	TRANSFER / DISCLOSURE AUTHORISED BY
	Transfer	Disclosure			

SAMPLE PRIVACY WARNING FOR FAX AND EMAIL

Email

The information contained in this email message, including any attachments is intended for the named addressee only. If you are not the intended recipient you must not copy, forward, distribute, take any action reliant on, or disclose any details of the information in this email to any other person or organisation. If you have received this email in error please notify us immediately.

Fax

The information contained in this fax message is intended for the named addressee only. If you are not the intended recipient you must not copy, distribute, take any action reliant on, or disclose any details of the information in this fax to any other person or organisation. If you have received this fax in error please notify us immediately.

IMPORTANT INFORMATION ABOUT THE PRACTICE AND YOUR PRIVACY

From 12 March 2014, new privacy laws – known as the Australian Privacy Principles (APPs) – commenced operation. The APPs apply across Australia and regulate how the practice handles your personal information. The APPs operate in addition to any State privacy legislation applicable to the practice.

To enable the practice to continue to deliver and enhance the products and services it provides, the practice holds personal information about you including information about your health. We recognise and support your right to privacy in relation to this information and will continue to handle it with care and in accordance with our professional and legal obligations.

The practice staff will continue to demonstrate integrity and understanding by protecting and keeping secure your personal and health information.

We ask you to read the practice's privacy information, including our Privacy Policy, and we invite you to contact our Privacy Officer if you have any questions.

Signed:
_____

Date: _____ / _____ / _____

Email:
_____

Telephone:
_____

Facsimile:
_____

Mail: The Privacy Officer

_____

_____

Your Health Information - Privacy Consent Form

Our practice respects your right to privacy and it has systems and processes in place to ensure it complies with the Australian Privacy Principles (APPs). The practice privacy policy is available on request.

Our practice [**insert company name of practice and ABN**] trading as [**insert trading name of practice**] collects information about you for the purpose of providing health services to you. In addition, personal information such as your name, address and health insurance details are used for the purpose of addressing accounts to you, as well as processing payments and writing to you about our services and any issues affecting your health care. We may collect information about you from third parties providing the collection of that information is necessary to provide you with health care.

We may disclose your health information to other health care professionals, or require it from them if, in our judgement, it is necessary in the context of your care.

We may also use parts of your health information for research purposes, in study groups or at seminars; however, in such situations, your personal identity will not be disclosed without your consent.

If you choose not to provide us with information relevant to your care, we may not be able to provide a service to you, or the service we are asked to provide may not be appropriate for your needs. Importantly, if you do not provide information that may be relevant to your care or that is otherwise requested by us, you could suffer some harm or other adverse outcome.

Your medical history, treatment records, x-rays and any other material relevant to your care will be stored by the practice. The practice privacy policy sets out how you can access your records or seek correction of your records.

The practice privacy policy sets out how you may complain about a breach of privacy and how the practice will deal with such a complaint.

As part of its electronic records system, the practice may rely on cloud storage providers located outside Australia. The practice will take reasonable steps to ensure that any offshore transfer complies with its obligations under the APPs.

The practice Privacy Officer can be contacted at the practice during business hours if you have any concerns or questions about a privacy matter.

Please sign this form as confirmation that you have read and understood the above information and consent to the collection and use of your health information.

Signed: _____

Date: _____

Patient/ Parent / Guardian Name:_____

Dependents:_____

ADA VICTORIA

THE PRACTICE PRIVACY POLICY FOR ONGOING CONTACT

This practice collects your personal information to assist us in providing the goods or services you have requested and to improve our products and services. We may be in touch to let you know about goods, services or promotions which may be of interest to you. Please let us know if you object to this and if you would prefer not to be contacted with special offers or in relation to our other goods and services. You can do this by letting the Privacy Officer know by any of the following methods:

Email	:	_____
Telephone	:	_____
Facsimile	:	_____
Mail	:	The Privacy Officer
		_____
		_____

You can gain access to your personal information
by contacting the Privacy Officer.

REQUEST FOR ACCESS TO OR CORRECTION OF PATIENT RECORDS

Please print all responses

PATIENT'S NAME		D.O.B.
NAME OF PERSON REQUESTING ACCESS/CORRECTION		RELATIONSHIP TO PATIENT _____
ADDRESS		
PHONE NO.		
EMAIL		
REQUEST		
Please tick form of access requested	o Inspection o Copy o Explanation or accurate summary o Correction	Depending on the type of access you request you may be charged a fee in accordance with applicable laws.
Please describe the records to which access is requested or what correction is requested		
Patient Signature		**Date:**
PRACTICE USE ONLY		
Access approved	Yes o No o	
Comments if declined		
Authorisation Signature		**Date:**

See also our Practice Privacy Policy

PATIENT/GUARDIAN AUTHORITY TO TRANSFER RECORDS TO ANOTHER PRACTICE

Dr …….. has explained to me the reasons for transferring information about ……(insert name of patient) to:

……

……(insert name and address of recipient practice).

I understand the explanation provided and hereby give my consent for this information to be released for the purpose(s) of:

……

Signature of patient/guardian: ……..

Date: ……/……/…….

Signature of dental practitioner: ……..

RESPONSE TO PATIENT REQUEST FOR TRANSFER OF FILE

Date

Patient name
Patient address

Dear

On **(date)** we received a request from you to transfer your file to **(insert new practice name)** located at **(insert new practice address)**.

To ensure we are transferring the health information to the correct practice we request you complete the attached form **(Patient/Guardian Authority to Transfer Records to Another Practice)** and return to us by post or in person.

Once we have received the form, we will contact (**insert new practice name**) to arrange transfer of your file.

(Alternative 1 – to be used in where the file must be copied and the file size is large) Due to the size of your file and the administrative time and cost in complying with your request we ask that you pay a small fee. This fee is set in accordance with relevant privacy laws.

We ask that you pay $_____ prior to us copying your file. This payment may be made by credit card over the phone, by cheque, or in person.

If you have any questions please feel free to contact me.

Yours sincerely

(name, position, contact details)

[NOTE – The amount that may be charged varies between jurisdictions. In Victoria, certain caps apply to the fees that may be charged. The table on the following page sets out the maximum fees that may be charged.
If your practice is located outside Victoria, you should determine if any caps apply before setting a fee.]

THIS TABLE IS FOR GUIDANCE ONLY – IT SHOULD NOT BE SENT TO THE PATIENT

The maximum fees that can be charged by practices in Victoria for the copying or transfer of health information (such as dental records) are set under the **Health Records Regulations 2012 (Vic).** See www.health.vic.gov.au/healthrecords/regs.htm

The maximum fees applicable in Victoria are:

Item	Fee cap
Items 1 & 2 (Schedule 1): Time for supervising inspection or viewing of records	1.2 fee unit (currently equal to $15.00) per half hour or part thereof**
Use of equipment not in organisation's possession	Reasonable costs incurred
Item 3: (a)&(b) **Copy** of health information to individual	**20 cents per page** for A4 black & white Reasonable costs otherwise
(c) Time for **assessing & collating** health information	**2.5 fee units ($31.30)**
(d) Transporting records held off site	1.2 fee units ($15.00)
(e) Postage	Actual postage cost, if request to be posted
Item 4: Providing an **accurate summary** of information to individual	Greater of usual consultation fee (if a health service provider) or 2.9 fee units per quarter hour ($36.30), up to 9.4 fee units ($117.80)
Item 1 (Schedule 2) **Copy** of health information to **another health service provider**	20 cents per page for A4 black & white if at least 20 pages Reasonable costs otherwise
Item 2: **Summary** of health information to another health service provider	Greater of usual consultation fee or 2.9 fee unit per quarter hour ($36.30), up to 9.4 fee units ($117.80), where the time taken to prepare is at least 30 minutes
Regulation 7: Functions of nominated health service provider under s. 42 of the Act	Reasonable costs not exceeding 4.7 fee units per quarter hour ($58.90) up to 23.6 fee units ($295.70)

The Health Records Regulations 2012 (Vic) set caps on fees for individuals seeking access to their health information in a manner other than by obtaining a copy or having their health information sent to a new provider. If such requests are made, consideration must be given to the fee caps that apply to the type of access sought.

RESPONSE TO DENTAL PRACTICE REQUESTING TRANSFER OF PATIENT FILE

Date

Name of Dental Practice to release patient file
Address of Dental Practice to release patient file

Dear **(dental practitioner)**

Re: Patient name, Date of birth, Patient address

We have received a request to transfer you a copy of the above mentioned patient's dental health record, which is attached.

To ensure we are transferring the health information to the correct practice, we request you acknowledge receipt of these files.

Yours sincerely

(name, position, contact details)

✂----------

I, Dr _____ am in receipt of

_____'s patient health record.

Signature: _____ Date: _____

PATIENT AUTHORITY TO TRANSFER RECORDS FROM ANOTHER PRACTICE

Dear (insert patient's name)

In providing the most appropriate dental treatment for you in our practice, we believe it would be of great assistance to access information about your previous treatment from

……(insert name of previous practice)

To ensure compliance with the Federal and State Privacy Legislation, we require your signed consent to authorise access to these records.

Please be aware that practitioners are entitled to charge fees to a patient requesting access to, and copies of, written records and other forms of diagnostic records, such as x-rays.

We have been advised that ……(insert name of transferring practice) will charge……..(insert amount or no charge) to transfer your records to us.

PATIENT CONSENT

I give permission for Dr …… to seek copies of my dental records from ……

I agree to pay the fee set out above associated with obtaining copies of my dental record.

Signature: ……

Name: ……..

Date: ……../……../……

PATIENT REPRESENTATIVE'S AUTHORITY TO REQUEST RECORDS FROM ANOTHER PRACTICE

Dear (patient's representative)

In providing the most appropriate dental treatment for (name of patient) in our practice, we believe it would be of great assistance to access information about (name of patient)'s previous treatment from ……

To ensure compliance with the Federal and State Privacy Legislation, we require your signed consent to authorise access to these records.

Please be aware that practitioners are entitled to charge fees to a patient requesting access to, and copies of, written records and other forms of diagnostic records, such as x-rays.

We have been advised that ……..(insert name of transferring practice) will charge……..(insert amount or no charge) to transfer your records to us.

CONSENT

I give permission for Dr …… to seek copies of

…….(name of patient)' dental records from

……

I agree to pay the fee set out above associated with obtaining copies of the relevant dental records.

Signature: ……

Name: ……..

Date: ……../……../……

LETTER TO PATIENTS RE SALE / TRANSFER / CLOSURE OF DENTAL PRACTICE

The following text may be edited for use as a letter of advice to patients currently involved in a course of care at the practice. Victorian and Tasmanian Practitioners should consult HPP 10 of the Victorian Health Records Act and the associated guidelines for direction on which patients should be sent this notice. (See also Section 4.1.9 – Practice Notice and Section 3)

Dear (insert patient name)

Dr …… wishes to announce the sale / transfer / closure of his/her dental practice located at ……[**insert address**]……..

If sold/transferred

The practice has been sold / transferred to Dr …….. (or alternative business name) effective from ….[**insert date**]….., and he / she / they will be pleased to continue providing your dental care. The previous owner has retired / relocated and extends appreciation to all patients who attended for treatment over the years.

Your records

Dental records held by the practice will be: [**insert whichever is appropriate**]

- transferred to Dr.....[**insert name or alternative business name**].....on [**insert date at least 21 days after letter sent to patient**]; or
- retained in the possession of Dr [**insert name of original dentist**].

If you would like your dental records to be transferred to another dentist or practice, please contact [**insert name of contact**].

If closed

The practice has been closed due to the retirement / ill health / death of the principal,…(insert name…). In future, you may wish to seek your dental care from …[**insert name of dentist or practice]**.....

Your records

Dental records held by the practice will be: [**insert whichever is appropriate**]

- transferred to Dr.....[**insert name or alternative business name**].....on [**insert date at least 21 days after letter sent to patient**]; or
- retained in the possession of Dr [**insert name of original dentist or alternative name**].

If you would like your dental records to be transferred to another dentist or practice, please contact [**insert name of contact**].

PRACTICE PRIVACY PROVISIONS

POLICY

The practice recognises and supports the right of all patients and staff to privacy and confidentiality of their personal records.

This practice has adopted as part of its Policies and Procedures a formal Privacy Policies and Procedures Manual.

All staff, agents and service providers are required to read, understand and adhere to the practice's policies and procedures. Breaches of the policies or procedures will be dealt with in accordance with the Practice policies and may result in disciplinary action including termination of employment/engagement.

Staff must maintain Patients' Privacy

Staff members are required to sign an Employee Undertaking for the Protection of Personal Information. The undertaking prohibits staff from discussing or reviewing patients' files or details for any reason other than in the performance of their duties.

Staff must also be aware that a breach of privacy law can occur by allowing a third party to gain access by either seeing or hearing information that they are not entitled to.

If a staff member feels it necessary to consult with another staff member for advice or a second opinion on a claim, they must do so discreetly. Staff members must not openly discuss patients or patient information where their conversation could be overheard by a member of the public. Staff are reminded that even if patient names are not discussed, the nature of a patient's condition may reveal their identity. Staff should ensure that when asking questions or discussing information with any person (including a patient) that care is taken to ensure a third party cannot hear the questions or the answers to those questions.

Staff must ensure that when they are providing information to a patient that the information provided is about that patient only and that there is no information about another person.

If patients require a copy of their records held by the practice, they will only be issued to them following receipt of a request in writing signed by the patient. The records will be sent by registered mail marked private and confidential and addressed to the patient. The request for such information may take up to 7 days to process. Requested information will be provided in hardcopy form and no patient will be given access to a terminal or screen to view their information. In some situations, a patient may be refused access or provided with an explanation of their records by a dentist.

Any requests for access to records or transfer of records must be referred to the practice Privacy Officer.

Where staff members are dealing with a patient either at the counter or over the telephone they must be discreet in their discussions. They may not speak out across the office or on hands free mode on the telephone.

If a patient at the counter is hard of hearing the requested information or the comments to be made should be written out so that the patient is not embarrassed or made feel that their information is not being respected at all times.

Staff with access to the Personally Controlled Electronic Health Record and Individual Healthcare Identifiers are reminded that they are subject to additional obligations of privacy and that misuse of these systems may constitute a criminal offence. Staff should consult with the practice Privacy Officer if they have any questions about their personal obligations.

No staff member or other person with access to practice information is permitted to comment or post any material on the internet, such as through social media sites that could reveal patient information or the services received by a patient. Staff and contractors are also forbidden from making or posting online comments that may bring the practice into disrepute or give rise to a complaint against the practice. Any breach of these provisions may result in disciplinary action, including termination of employment/engagement.

Last Reviewed: ____ / ____ / _____

EMPLOYEE UNDERTAKING FOR THE PROTECTION OF PERSONAL INFORMATION

VICTORIA

As an employee of this practice I have read the practice's Privacy Policy, the Overview of Privacy document, discussed with the practice Privacy Officer the importance of privacy and provide this undertaking as follows:

I _____ an employee of _____

acknowledge that I am prohibited from discussing or reviewing patients' files or details for any reason other than in the performance of my duties.

I am aware of the practice's Standard Operating Procedures on Privacy Provisions and accept the need to adhere to their requirements.

I understand that a breach of patient privacy may result in significant consequences for me and the practice, and that if I am in breach of the practice's policies and procedures regarding patient privacy, disciplinary action may be taken against me and my employment may be terminated.

Signed: _____

Date: _____ / _____ / _____

EMPLOYEE UNDERTAKING FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

Employees are in possession of and have access to a broad variety of personal and commercial information that is confidential. Inappropriate release of that information could be injurious to individuals and **[insert name of Dental Practice].** All employees have an obligation to actively protect and safeguard confidential information in a manner designed to prevent its unauthorized disclosure.

Confidential information is defined as any information that forms part of the practice's personnel, financial or operational business records, or marketing and business plans. Confidential information includes, but is not limited to:

1. Records or information relating to the practice's finances and billing practices.

2. Any records or information relating to practice staff members, medical staff credentialing, discipline, or other peer review activities, including comments regarding appropriateness or necessity of care to a patient rendered by a practitioner.

3. Any records, information, or data relating to the practice's strategic, marketing, or business plans.

4. Any records or information related to a pending, threatened, or potential lawsuit or any administrative, civil, criminal or other legal claim by or against the practice.

I, _____ (print employee name) understand that:

1. unless disclosure is legally required of me or is required in the course of my employment, under no circumstances may I discuss or disclose any confidential information. This includes disclosures or discussions on social media sites such as Facebook.

2. violation of this agreement will be grounds for immediate termination and/or legal action being brought against me.

By signing this undertaking I understand that it does not create any contractual or other right to continued employment nor does it repeal or replace the employment and privacy policies of the practice.

Signed for and on behalf of [**Insert name of THE DENTAL PRACTICE]** by **[Insert name of Employer/Practice Manager]**

_____

SIGNED by (**name of employee)**_____

Date _____

Witnessed by:_____ (print name _____)

Date _____

PRACTICE PRIVACY HANDLING FRAMEWORK

The practice's Privacy Officer will review all complaints and any breaches of patient privacy – whether the breach is notified to the practice or discovered internally.

All cases of actual or suspected privacy breaches will be dealt with in accordance with the “Guide to handling personal information security breaches” published by the Office of the Australian Information Commissioner (**OAIC**) or other applicable guides published by the OAIC.

All actual or possible privacy breaches will be brought to the attention of the practice Privacy Officer and the practice's Principal for review and recommendations.

Following OAIC guidance, breaches of privacy may be referred to the OAIC or relevant State health commissioner for review. In general, serious breaches of patient privacy that could give rise to a “real risk of serious harm” will be referred.

Staff Breaches of privacy policies and procedures

Where there is a breach of practice policy and procedure by a staff member, the matter will be reviewed by the Privacy Officer and the practice’s Principal.

The practice regards any breach of patient privacy as a serious matter that could give rise to disciplinary action including termination of employment.

If the practice reasonably believes a staff member has committed an offence concerning patient information, the appropriate authorities will be notified.

PRACTICE PRIVACY COMPLIANTS REGISTER

Date & Time Complaint Received	Name & Contact Details of Complainant	Details of the Complaint or Incident	Action Taken or Comments Passed to Date	Name of the Recording Officer

PRIVACY AND THE PRACTICE'S EMPLOYEE RECORDS EXEMPTION

The *Privacy Act 1988* (Privacy Act) deals with employee records and health records differently.

As an employee, the handling of your personal information by the practice is exempt from the Privacy Act if it is directly related to:

1. your current or former employment relationship; or

2. an employee record relating to you.

This means that the practice does not need to comply with the Australian Privacy Principles in the Privacy Act when it handles current and past employee records. In particular, this means that under the Privacy Act, the practice does not have to grant you access to your employee records.

STAFF TELEPHONE PROTOCOL TO CONFIRM IDENTITY OF PERSON SEEKING INFORMATION

When a patient telephones the practice to request that information be provided on their behalf to another dental practice, the patient should be asked to sign a written authority to do so. If the patient cannot visit the practice, an authority form could be mailed and returned to the practice. Before sending information to the recipient practice, staff should verify that the recipient practice is expecting the patient's record. If the request is valid, copies of records should be sent directly to the recipient practice (rather than giving them to the patient).

Similarly, a patient's request for access to their records should be put in writing. If the patient makes phone contact, encourage them to complete the appropriate form and provide assistance as required (for example posting a copy of the form). Once the request is received, the patient should be contacted to verify the request has been sent by them – and a copy of records should not be sent to the patient by mail unless absolutely necessary and the identity and address of the patient is certain.

SAMPLE APPROACH

A patient calls and asks for records to be mailed to them.

1. Ask for his/her name and address and explain that you will place him/her on hold while you locate his/her records.

2. *(Upon your return to the telephone, having checked this person is a patient of the practice, and with records in hand,)*
   Explain your practice policy on privacy requires you to have such a request in writing, and would he/she be able to attend the practice to sign an authority form. *(If there is a reason for the patient not attending in person and he/she requires the authority to be mailed, explain the process including the need to verify the request once received by the practice)*

3. If the patient becomes angry and refuses to co-operate, explain the privacy policy is designed to protect the information you have collected about them, and that you don't want to release it to anyone who is not entitled to have it.

5. If the patient remains angry, suggest you take a contact number and ask the dentist to return his/her call.

6. On making a return call, the dentist should stress the need to ensure the correct information is given to the correct person. Offers of assistance should be made such as sending the appropriate form with a stamped return self-addressed envelope. The dentist should enquire whether the patient is seeking access or a transfer of their information to another practice and seek to facilitate that transfer.

MOBILE DEVICE POLICY

VICTORIA

Introduction

To assist practitioners and key staff members or contractors, such as the Practice Manager/Practice Principal in the execution of their roles and responsibilities they have been supplied with mobile devices such as mobile phone, laptop, or "tablet computer". It is the expectation of these staff that they will protect the security of these devices and the data contained in them whilst in their possession.

Staff or contractors using their own mobile device for remote access will also abide by this policy whenever connected to the practice computer network.

Policies and Procedures

1. All mobile devices supplied to staff or contractors to assist them in carrying out their duties and responsibilities remain the property of the practice and are to be returned on termination of employment or contract.
2. All staff or contractors supplied with a mobile device will be required to sign a copy of this policy agreeing to the terms and conditions.
3. Access and permissions through the mobile device will be determined by the Information Security Officer (ISO).
4. A keypad lock is to be implemented on all mobile devices as a security measure to protect data contained on the device. The code is to be disclosed to the ISO. Should the staff member/contractor change the code they are to inform the ISO immediately.
5. No mobile device is to be left unattended in a car, public area of the practice, in an unattended area of the practice (including a surgery not in use) or public location such as a cafe.
6. If the mobile device is left at home it is to be switched off or switched to silent so it does not attract the attention of would be thieves.
7. If the device is lost or stolen the Police, ISO and Practice Principal are to be notified immediately.
8. At no time is media, software or hardware to be loaded onto the device without the express permission of the ISO or Practice Principal.
9. The mobile device is only for practice work use, not personal use unless there is a written agreement in place to this effect.
10. The ISO will ensure that all device serial numbers are recorded for insurance purposes.
11. The device is not to have Bluetooth switched on permanently as a security measure as this is a quick and easy way for "hackers" to gain access to practice data. This can even occur from several kilometres away with the right software.
12. The device is not to be connected to unprotected wireless access points or "internet hotspots" as "hackers" open up hotspots to attract users and steal data.
13. The device must remain password protected.

I _____agree to abide by these terms and conditions.

Signed_____Date_____

ISP Privacy Letter

Dear (name of ISP),

In order to prepare an accurate statement about privacy issues for publication on the practice's website, and thereby to ensure our compliance with State and Federal Privacy laws, I am writing to seek your responses to the following key questions.

1. ISP's full business name.

_____

2. What information do you record for statistical purposes, e.g. date and time of visit, pages accessed, server address etc?

_____

_____

3. How often do you provide information to us, and in what form?

_____

_____

4. Are security measures used, such as encryption, secure sockets layer (etc.) used, and if so, what level of security is available, to allow for secure Internet communication?

_____

_____

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

_____

_____

Thank you for your assistance with this compliance activity.

Signature block

LETTER TO DENTAL LABORATORY REQUESTING COMMITMENT TO APPs

Dear (Laboratory owner)

You will be aware of requirements under the Privacy Act and applicable State laws concerning patient confidentiality.

Given that our practice is required to comply with the Australian Privacy Principles and we transfer patient information to you, we are keen to ensure your organisation also complies with the Australian Privacy Principles.

To this end, we ask that you sign the statement below and return the original to us for our files.

Thank you for your assistance with this compliance activity.

Signature block

LABORATORY COMMITMENT

I (Laboratory owner's name), owner of the (name of dental laboratory) acknowledge that (insert name of dental laboratory) is bound to comply with the Australian Privacy Principles and has systems, policies and procedures in place to ensure compliance.

Signature: ……..

Name of Laboratory owner: …….

Name of Laboratory: …….

Date: ……

LETTER TO SERVICE ENTITIES REQUESTING COMMITMENT TO THE AUSTRALIAN PRIVACY PRINCIPLES

Dear (name of owner/manager of service provider)

You will be aware that our practice is bound to comply with the Australian Privacy Principles regarding the protection of health information.

Given your involvement in providing services to our practice we are keen to ensure your organisation also complies with the Australian Privacy Principles.

We would be grateful if you would sign the statement below and return the original to us for our files.

Thank you for your assistance with this compliance activity.

Signature block

COMMITMENT

I (name of owner/manager), owner/manager of the (service provider's name) have read and understood the Australian Privacy Principles and confirm that (service provider's name) has systems, policies and procedures in place to ensure compliance with the principles.

Signature: ……..

Name of service provider's owner/manager: …….

Name of service provider: …….

Date: …….

LETTER OF REFERRAL
ATTACHING RECORDS ABOUT THE PATIENT

VICTORIA

See the updated Referral Form on the Practice+ Resources page at www.adavb.net.

LETTER TO OTHER PRACTICE SEEKING ACCESS TO PATIENT INFORMATION AND REQUESTING PATIENT CONSENT

Dear (other practice)

Thank you for your request for access to a copy of records of our treatment of (patient's name) _____.

As a professional courtesy we would be pleased to assist with a **copy** of our original records (of course originals are always retained at the practice); however, we require consent of the patient for transfer.

To that end, we request that you obtain the patient's signed consent to your request using the format supplied below or a suitable equivalent. We are happy to receive the signed consent by fax.

Thank you for your assistance.

Signature block (include fax number)

PATIENT CONSENT

I give permission for Dr …… to obtain copies of (name of patient)' dental records from ……

(**Delete if not applicable**) I agree to pay the following fee incurred in the copying process as specified in the *Health Records Regulations 2012* (Vic):……

Signature: ……

Name: ……..

Date: ……../……../……

LETTER TO OTHER PARTY REQUESTING ACCESS TO PATIENT INFORMATION

(Letter to be sent after confirming the cost of transferring files from the transferring practice and completing form 4.2.6 or 4.2.7 which should then be attached to this letter)

Dear (other party)

(patient's name) has consulted this practice for on-going dental treatment. We understand that you hold records pertaining to (patient's name) previous treatment.

To assist us in providing the most appropriate treatment, we ask for your help in supplying a copy of relevant records and radiographs.

From our previous telephone contact we understand that you will charge (insert amount or state will not charge) to transfer the requested files.

The patient's signed authority to transfer records is attached. (**REFER TO 4.2.6 OR 4.2.7**)

We hope to schedule an appointment for (patient's name) within the next few weeks, and would therefore appreciate your acceding to this request within the next week if possible. If you foresee problems in providing assistance, please contact us at your earliest convenience.

Thank you for your assistance.

Signature block

APPENDIX 1

Extracts from the *Privacy Act 1988* (Cth)

Schedule 1—Australian Privacy Principles

Overview of the Australian Privacy Principles

Overview

This Schedule sets out the Australian Privacy Principles.

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Australian Privacy Principles

The Australian Privacy Principles are:

Australian Privacy Principle 1—open and transparent management of personal information

Australian Privacy Principle 2—anonymity and pseudonymity

Australian Privacy Principle 3—collection of solicited personal information

Australian Privacy Principle 4—dealing with unsolicited personal information

Australian Privacy Principle 5—notification of the collection of personal information

Australian Privacy Principle 6—use or disclosure of personal information

Australian Privacy Principle 7—direct marketing

Australian Privacy Principle 8—cross-border disclosure of personal information

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Australian Privacy Principle 10—quality of personal information

Australian Privacy Principle 11—security of personal information

Australian Privacy Principle 12—access to personal information

Australian Privacy Principle 13—correction of personal information

Part 1—Consideration of personal information privacy

1 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.

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.

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;

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

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

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

(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;

(f) whether the entity is likely to disclose personal information 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.

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.

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.

2 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.

Part 2—Collection of personal information

3 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.

4 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.

5 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.

Part 3—Dealing with personal information

6 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.

7 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.

8 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.

9 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).

Part 4—Integrity of personal information

10 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.

11 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.

Part 5—Access to, and correction of, personal information

12 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.

13 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).

Additional Extracts from the Privacy Act 1988 to assist in interpretation of the APPs

Definition of personal information

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.

Definition of sensitive information

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; or

(c) genetic information about an individual that is not otherwise health information.

Section 16A - Permitted general situations in relation to the collection, use or disclosure of personal information

(1) A ***permitted general situation*** exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:

(a) the entity is an entity of a kind specified in an item in column 1 of the table; and

(b) the item in column 2 of the table applies to the information or identifier; and

(c) such conditions as are specified in the item in column 3 of the table are satisfied.

Permitted general situations

Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
1	APP entity	(a) personal information; or (b) a government related identifier.	(a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	APP entity	(a) personal information; or (b) a government related identifier.	(a) 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; and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	APP entity	Personal information	(a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and (b) the collection, use or disclosure complies with the rules made under subsection (2).
4	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence

Permitted general situations			
Item	**Column 1** **Kind of entity**	**Column 2** **Item applies to**	**Column 3** **Condition(s)**
			of a legal or equitable claim.
5	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.
6	Agency	Personal information	The entity reasonably believes that the collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities.
7	Defence Force	Personal information	The entity reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories: (a) war or warlike operations; (b) peacekeeping or peace enforcement; (c) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

(2) The Commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table in subsection (1).

Section 16B - Permitted health situations in relation to the collection, use or disclosure of health information

Collection—provision of a health service

(1) A ***permitted health situation*** exists in relation to the collection by an organisation of health information about an individual if:

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

(b) either:

(i) the collection is required or authorised by or under an Australian law (other than this Act); or

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

Collection—research etc.

(2) A ***permitted health situation*** exists in relation to the collection by an organisation of 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 about the individual that is de-identified information; and

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

(d) any of the following apply:

(i) the collection is required by or under an Australian law (other than this Act);

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

(iii) the information is collected in accordance with guidelines approved under section 95A for the purposes of this subparagraph.

Use or disclosure—research etc.

(3) A ***permitted health situation*** exists in relation to the use or disclosure by an organisation of health information about an individual if:

(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the organisation to obtain the individual's consent to the use or disclosure; and

(c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes of this paragraph; and

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

Use or disclosure—genetic information

(4) A ***permitted health situation*** exists in relation to the use or disclosure by an organisation of genetic information about an individual (the ***first individual***) if:

(a) the organisation has obtained the information in the course of providing a health service to the first individual; and

(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and

(c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and

(d) in the case of disclosure—the recipient of the information is a genetic relative of the first individual.

Disclosure—responsible person for an individual

(5) A ***permitted health situation*** exists in relation to the disclosure by an organisation of health information about an individual if:
  (a) the organisation provides a health service to the individual; and
  (b) the recipient of the information is a responsible person for the individual; and
  (c) the individual:
    (i) is physically or legally incapable of giving consent to the disclosure; or
    (ii) physically cannot communicate consent to the disclosure; and
  (d) another individual (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
  (e) 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
  (f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Section 16C - Acts and practices of overseas recipients of personal information

(1) This section applies if:
  (a) an APP entity discloses personal information about an individual to an overseas recipient; and
  (b) Australian Privacy Principle 8.1 applies to the disclosure of the information; and
  (c) the Australian Privacy Principles do not apply, under this Act, to an act done, or a practice engaged in, by the overseas recipient in relation to the information; and
  (d) the overseas recipient does an act, or engages in a practice, in relation to the information that would be a breach of the Australian Privacy Principles (other than Australian Privacy Principle 1) if those Australian Privacy Principles so applied to that act or practice.

(2) The act done, or the practice engaged in, by the overseas recipient is taken, for the purposes of this Act:
  (a) to have been done, or engaged in, by the APP entity; and
  (b) to be a breach of those Australian Privacy Principles by the APP entity.

Appendix 2
Health Privacy Principles
Extracts from the Health Records Act 2001 (Vic)

SCHEDULE 1

Section 19

THE HEALTH PRIVACY PRINCIPLES

1 Principle 1—Collection
When health information may be collected

1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies—

(a) the individual has consented;

(b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law);

(c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent within the meaning of section 85(3) and—

(i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(ii) the individual does not have such an authorised representative;

(d) the information is disclosed to the organisation in accordance with HPP 2.2(a), (f), (i) or (l) or HPP 2.5;

(e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest—

(i) 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

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

(iii) the information is collected in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this subparagraph;

(f) the collection is necessary to prevent or lessen—

(i) a serious and imminent threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare—

and the information is collected in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph;

(g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function;

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

(i) the collection is in the prescribed circumstances.

How health information is to be collected

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

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

1.4 At or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects health information about an individual from the individual, the organisation must take steps that are reasonable in the circumstances to ensure that the individual is generally 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) to whom (or the types of individuals or 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.

1.5 If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is or has been made aware of the matters listed in HPP 1.4 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 or would involve the disclosure of information given in confidence[i].

1.6 An organisation is not required to notify the individual of the identity of persons, or classes of persons, to whom health information may be disclosed in accordance with HPP 2.2(f).

Information given in confidence[ii]

1.7 If personal information is given in confidence to a health service provider about an individual by a person other than—

(a) the individual; or

(b) a health service provider in the course of, or otherwise in relation to, the provision of health services to the individual—

with a request that the information not be communicated to the individual to whom it relates, the provider must—

(c) confirm with the person that the information is to remain confidential; and

(d) if the information remains confidential—

(i) record the information only if it is relevant to the provision of health services to, or the care of, the individual; and

(ii) take reasonable steps to ensure that the information is accurate and not misleading; and

(e) take reasonable steps to record that the information is given in confidence and is to remain confidential.

2 Principle 2—Use and Disclosure[iii]

2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1.

2.2 An organisation must not use or disclose health information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies[iv]—

(a) both of the following apply—

(i) the secondary purpose is directly related to the primary purpose; and

(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) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); or

(d) all of the following apply—

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and

(iii) the individual is incapable of giving consent within the meaning of section 85(3) and—

(A) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(B) the individual does not have such an authorised representative; or

(e) all of the following apply—

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and

(iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and

(iv) the information is used in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(f) the use or disclosure is for the purpose of—

(i) funding, management, planning, monitoring, improvement or evaluation of health services; or

(ii) training provided by a health service provider to employees or persons working with the organisation—

and—

(iii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the individual's consent to the use or disclosure; or

(iv) reasonable steps are taken to de-identify the information—

and—

(v) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(vi) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this subparagraph; or

(g) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest—

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

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

(iii) the use or disclosure is in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this subparagraph; and

(iv) in the case of disclosure—

(A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and

(B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or

(h) 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, safety or welfare; or

(ii) a serious threat to public health, public safety or public welfare—

and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(i) [v]the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(j) [vi]the organisation reasonably believes that the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(k) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(l) the use or disclosure is in the prescribed circumstances.

Note

Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

2.3 If an organisation discloses health information under paragraph (i) or (j) of HPP 2.2, it must make a written note of the disclosure.

2.4 Despite HPP 2.2, a health service provider may disclose health information about an individual to an immediate family member of the individual if—

(a) either—

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

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

(b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (a); and

(c) the individual is incapable of giving consent to the disclosure within the meaning of section 85(3); and

(d) the disclosure is not contrary to any wish—

(i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and

(ii) of which the organisation is aware or could be made aware by taking reasonable steps; and

(e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

2.5 Despite HPP 2.2, an organisation may use or disclose health information about an individual where—

(a) it is known or suspected that the individual is dead; or

(b) it is known or suspected that the individual is missing; or

(c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure—

and the use or disclosure is to the extent reasonably necessary—

(d) to identify the individual; or

(e) to ascertain the identity and location of an immediate family member or other relative of the individual for the purpose of—

(i) enabling a member of the police force, a coroner or other prescribed organisation to contact the immediate family member or other relative for compassionate reasons; or

(ii) to assist in the identification of the individual—

and, in the circumstances referred to in paragraph (b) or (c)—

(f) the use or disclosure is not contrary to any wish—

(i) expressed by the individual before he or she went missing or became incapable of consenting and not withdrawn by the individual; and

(ii) of which the organisation is aware or could have become aware by taking reasonable steps; and

(g) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph.

3 Principle 3—Data Quality

3.1 An organisation must take steps that are reasonable in the circumstances to make sure that, having regard to the purpose for which the information is to be used, the health information it collects, uses, holds or discloses is accurate, complete, up to date and relevant to its functions or activities.

4 Principle 4—Data Security and Data Retention

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

4.2 A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless—

(a) the deletion is permitted, authorised or required by the regulations or any other law; or

(b) the deletion is not contrary to the regulations or any other law and occurs—

(i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or

(ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider—

whichever is the later.

4.3 A health service provider who deletes health information in accordance with HPP 4.2 must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted.

4.4 A health service provider who transfers health information to another individual or organisation and does not continue to hold a record of that information must make a written note of the name and address of the individual or organisation to whom it was transferred.

4.5 An organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any

other purpose authorised by this Act, the regulations made under this Act or any other law.

5 Principle 5—Openness

5.1 An organisation must set out in a document—

(a) clearly expressed policies on its management of health information; and

(b) the steps that an individual must take in order to obtain access to their health information.

The organisation must make the document available to anyone who asks for it.

5.2 On request by an individual, an organisation must take reasonable steps—

(a) to let the individual know—

(i) whether the organisation holds health information relating to the individual; and

(ii) the steps that the individual should take if the individual wishes to obtain access to the information; and

(b) if the organisation holds health information relating to the individual, to let the individual know in general terms—

(i) the nature of the information; and

(ii) the purposes for which the information is used; and

(iii) how the organisation collects, holds, uses and discloses the information.

6 Principle 6—Access and Correction

Access[vii]

6.1 If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual in accordance with Part 5, unless—

(a) providing access would pose a serious threat to the life or health of any person under section 26 and refusing access is in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(b) providing access would have an unreasonable impact on the privacy of other individuals and refusing access is in accordance with

guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(c) the information relates to existing legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery in those proceedings[viii] or is subject to legal professional privilege or client legal privilege; or

(d) 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 in such a way as to expose the organisation unreasonably to disadvantage; or

(e) the information is subject to confidentiality under section 27; or

(f) providing access would be unlawful; or

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

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

(i) providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency; or

(j) a law enforcement agency 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; or

(k) 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

(l) the individual has been provided with access to the health information in accordance with Part 5 and is making an unreasonable, repeated request for access to the same information in the same way.

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 access to the information.

Note

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

6.3 If access is refused on the ground that it would pose a serious threat to the life or health of the individual, the procedure in Division 3 of Part 5 applies.

6.4 Without limiting sections 26 and 27, nothing in this Principle compels an organisation to refuse to provide an individual with access to his or her health information.

Correction

6.5 [ix]If an organisation holds health information about an individual and the individual is able to establish that the information is inaccurate, incomplete, misleading or not up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date but must not delete the information otherwise than in accordance with HPP 4.2.

6.6 If—

(a) the organisation is not willing to correct the health information in accordance with a request by the individual; and

(b) no decision or recommendation to the effect that the information should be corrected wholly or partly in accordance with the request, is pending or has been made under this Act or any other law; and

(c) the individual gives to the organisation a written statement concerning the requested correction—

the organisation must take reasonable steps to associate the statement with the information.

6.7 If the organisation accepts the need to correct the health information but—

(a) the organisation considers it likely that leaving incorrect information, even if corrected, could cause harm to the individual or result in inappropriate health services or care being provided; or

(b) the form in which the health information is held makes correction impossible; or

(c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so corrected—

the organisation must place the incorrect information on a record which is not generally available to anyone involved in providing health services to the individual, and to which access is restricted, and take reasonable

steps to ensure that only the corrected information is generally available to anyone who may provide health services to the individual.

6.8 If an organisation corrects health information about an individual, it must—

(a) if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made; and

(b) take reasonable steps to notify any health service providers to whom the organisation disclosed the health information before its correction and who may reasonably be expected to rely on that information in the future.

6.9 If an individual requests an organisation to correct health information about the individual, the organisation must take reasonable steps to notify the individual of a decision on the request as soon as practicable but in any case not later than 30 days after the request is received by the organisation.

Written reasons

6.10 An organisation must provide written reasons for refusal of access[x] or a refusal to correct health information.

7 Principle 7—Identifiers

7.1 An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

7.2 Subject to HPP 7.4, a private sector organisation may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if—

(a) the individual has consented to the adoption of the same identifier; or

(b) the use or disclosure of the identifier is required or authorised by or under law.

7.3 Subject to HPP 7.4, a private sector organisation may only use or disclose an identifier assigned to an individual by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if—

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more of paragraphs (c) to (l) of HPP 2.2; or

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

(c) the disclosure is to the public sector organisation which assigned the identifier to enable the public sector organisation to identify the individual for its own purposes.

7.4 If the use or disclosure of an identifier assigned to an individual by a public sector organisation is necessary for a private sector organisation to fulfil its obligations to, or requirements of, the public sector organisation, a private sector organisation may either—

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector organisation; or

(b) use or disclose an identifier of the individual that has been assigned by the public sector organisation.

8 Principle 8—Anonymity

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

9 Principle 9—Transborder Data Flows

9.1 An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria 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 Health Privacy Principles; or

(b) the individual consents to the transfer; or

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

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

(e) all of the following apply—

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

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

(iii) if it were practicable to obtain that 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 Health Privacy Principles; or

(g) the transfer is authorised or required by any other law.

10 Principle 10—Transfer or closure of the practice of a health service provider

10.1 This Principle applies if the practice or business of a health service provider (***the provider***) is to be—

(a) sold or otherwise transferred and the provider will not be providing health services in the new practice or business; or

(b) closed down.

10.2 The provider or, if the provider is deceased, the legal representatives of the provider, must—

(a) publish a notice in a newspaper circulating in the locality of the practice or business stating—

(i) that the practice or business has been, or is about to be, sold, transferred or closed down, as the case may be; and

(ii) the manner in which the provider proposes to deal with the health information held by the practice or business about individuals who have received health services from the provider, including whether the provider proposes to retain the information or make it available for transfer to those individuals or their health service providers; and

(b) take any other steps to notify individuals who have received a health service from the provider in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph.

10.3 Not earlier than 21 days after giving notice in accordance with HPP 10.2, the person giving the notice must, in relation to health information about

an individual held by, or on behalf of, the practice or business, elect to retain that information or transfer it to—

(a) the health service provider, if any, who takes over the practice or business; or

(b) the individual or a health service provider nominated by him or her.

10.4 A person who elects to retain health information must continue to hold it or transfer it to a competent organisation for safe storage in Victoria, until the time, if any, when the health information is destroyed in accordance with HPP 4.

10.5 Subject to HPP 10.2, a person must comply with the requirements of this Principle as soon as practicable.

10.6 Despite any other provision of the Health Privacy Principles, a person who transfers health information in accordance with this Principle does not, by so doing, contravene the Health Privacy Principles.

10.7 If—

(a) an individual, in response to a notice published under HPP 10.2, requests that health information be transferred to him or her or to a health service provider nominated by him or her; and

(b) the person who published the notice elects to retain the health information—

the request must be taken to be—

(c) in the case of a request that the health information be transferred to him or her, a request for access to that health information in accordance with Part 5 or HPP 6; and

(d) in the case of a request that the health information be transferred to a health service provider nominated by him or her, a request for the transfer of that health information in accordance with HPP 11—

and it must be dealt with in accordance with this Act.

10.8 This Principle operates subject to any other law, including the **Public Records Act 1973**.

10.9 For the purposes of HPP 10.1(a), a business or practice of a provider is transferred if—

(a) it is amalgamated with another organisation; and

(b) the successor organisation which is the result of the amalgamation is a private sector organisation.

11 Principle 11—Making information available to another health service provider

11.1 If an individual—

(a) requests a health service provider to make health information relating to the individual held by the provider available to another health service provider; or

(b) authorises another health service provider to request a health service provider to make health information relating to the individual held by that provider available to the requesting health service provider—

a health service provider to whom the request is made and who holds health information about the individual must, on payment of a fee not exceeding the prescribed maximum fee and subject to the regulations, provide a copy or written summary of that health information to that other health service provider.

11.2 A health service provider must comply with the requirements of this Principle as soon as practicable.

11.3 Nothing in Part 5 or HPP 6 limits the operation of this Principle.

11.4 For the purposes of HPP 10.7, this Principle applies to a legal representative of a deceased health service provider in the same way that it applies to a health service provider.

---

[i]Sch. 1 HPP 1.5: See HPP 1.7 and also section 27.

[ii]Sch. 1 HPP 1.7: See also section 27.

[iii]Sch. 1 HPP 2: See also HPP 9 for requirements relating to the transfer of health information to a person who is outside Victoria.

[iv]Sch. 1 HPP 2.2: A use or disclosure may be permitted under more than one paragraph of HPP 2.2.

[v] Sch. 1. HPP 2.2(i): For the purposes of this paragraph, the term "breach of confidence" relates to the general law of confidence (including but not limited to the common law or in equity), which requires, amongst other things, that a duty of confidence exists under that law which is not, in the particular circumstances, outweighed by any countervailing public interest under that law.

[vi] Sch. 1. HPP 2.2(j): For the purposes of this paragraph, the term "breach of confidence" relates to the general law of confidence (including but not limited to the common law or in equity), which requires, amongst other things, that a duty of confidence exists under that law which is not, in the particular circumstances, outweighed by any countervailing public interest under that law.

[vii]Sch. 1 HPP 6: See section 34(3) for access to health information, only part of which is claimed to fall within HPP 6.1 or 6.2.

[viii]Sch. 1 HPP 6.1(c): See also section 96.

[ix]Sch. 1 HPP 6.5: See HPP 4.2 and HPP 4.3 for deletion or destruction of health information.

[x]Sch. 1 HPP 6.10: See section 35 regarding refusal of access.

Appendix 3

Tasmanian Charter of Health Rights and Responsibilities

RIGHT 3 - CONFIDENTIALITY, PRIVACY AND SECURITY

The Rights of the Health Service Consumer

- The health service consumer has the right to have his/her personal health information and any matters of a sensitive nature kept confidential.

  No identifying information about the consumer, his/her condition or treatment may be disclosed without his/her consent unless the disclosure is required or authorised by law.

  In some cases, the provider is legally required to disclose health issues under mandatory reporting requirements or in the public interest.

- The right to be informed if the provider is required to disclose information about his/her health due to mandatory reporting requirements or in the public interest.
- The right to know who may have access to his/her personal health record, within the bounds of confidentiality.
- The right to know what sort of information is kept on his/her health record.
- The right to nominate another person who may receive information about the consumer's health status and care. This person does not necessarily have to be a next of kin.
- The right to have information about his/her health status and care passed on to another provider, at his/her request.
- The right to expect that staff of health service facilities are bound by confidentiality agreements, and will be disciplined if these agreements are breached.
- The right to health service facilities which ensure his/her privacy when receiving health care.
- The right to be treated with sensitivity as regards his/her confidentiality and privacy.
- The right to expect that information about his/her health is kept securely and cannot be easily accessed by unauthorised persons.
- Any record that contains personal information about the consumer's health should not be left in reception areas or treatment rooms. When the provider or another authorised person does not have a file, it should be stored securely. The same applies to computer or electronic records.
- Similarly, health service providers should not talk about consumer's health or care where other unauthorised persons can overhear them.

The Rights of the Health Service Provider

- The provider has the right to discuss the health care and treatment of a consumer with other providers for advice and support, in the best interest of the consumer's health and well-being.

APPENDIX 4

PRIVACY CONTACTS

For matters related to **Federal** Privacy legislation

Office of the Australian Information Commissioner
www.oaic.gov.au

ADA Inc.
www.ada.org.au

For matters related to **Victorian** Health Records legislation
Health Services Commissioner
Ph 8601 5222
www.health.vic.gov.au/hsc

For matters related to the **Tasmanian** Charter of Health Rights and Responsibilities

Health Complaints Commissioner
Ph 1800 001 170
www.healthcomplaints.tas.gov.au/home

For member enquiries regarding Privacy obligations of **Victorian** and **Tasmanian** dental practices

ADAVB Inc.
Ph (03) 8825 4600
www.adavb.net