SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS) – HEALTH SERVICE PROVIDERS

APP 1 Open and Transparent management of personal information

The practice must have an up to date and available privacy policy that covers specified information. The privacy policy must be made available to patients free of charge.

APP 2 Anonymity and Pseudonymity

Individuals must have the option of not identifying themselves, or using a pseudonym, unless impracticable or unlawful.

APP 3 Collection of solicited information

Sensitive information (including health information) must only be collected:

- with consent from the individual (or authorised guardian); and
- where reasonably necessary for the functions and activities of the practice (that is, the provision of health services).

Information should only be collected from the patient unless it is impracticable to do so.

Example: *Information about a patient's family member is collected while taking a history. This is acceptable if the information is reasonably necessary to treat the patient.*

APP 4 Dealing with unsolicited information

Where an entity receives personal information it did not solicit, it must determine whether the information could have been collected under APP 3. If not, the information must be de-identified or destroyed.

APP 5 Notification of collection of personal information

Individuals must be made aware of the nature of the personal information the practice collects. This includes information on:

- accessing and amending medical records
- how to make a complaint
- whether information will be used for direct marketing or disclosed to overseas recipients.

The practice's privacy and patient consent documents should cover these points.

APP 6 Use and disclosure of personal information

Information collected by the practice must only be used for a primary purpose or a secondary purpose directly related to the primary purpose, and only where the patient has provided consent to the use or disclosure.

A '**primary purpose**' is the reason the information was collected (for example, for the provision of health care)

A '**secondary purpose**' is a purpose ancillary but closely related to the primary purpose. For example, using patient details for billing purposes, or disclosing patient details to a specialist for referral.

Disclosure may also be required by law, including where there is a:

- warrant from Police to access medical records
- subpoena to produce document or give evidence
- obligation of mandatory notification of child abuse or notifiable disease.

Use or disclosure for a secondary purpose is also lawful in 'permitted general situations', without consent of the patient. These most relevant of these include:

- where necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public and it is unreasonable/impracticable to obtain the patient's consent. The threat need not be 'imminent' but it must be 'serious'.
- in instances of suspected or actual unlawful activity or serious misconduct that relates to the practice's functions and use or disclosure is necessary to take appropriate action.
- to locate a missing person – if the practice has a reasonable belief that the use or disclosure of personal information is reasonably necessary to locate a missing person. **Example:** *medical records indicate a 17 yr old male who has been reported missing was proposing to travel interstate to meet a girl he met on facebook.*

- to defend or establish a legal or equitable claim.
- to lawyers or insurers in response to complaints or claims.
- for confidential mediation/ADR processes – practices have the right to use or disclose patient information during a confidential alternative dispute resolution process such as mediation.

There are 3 'permitted health situations' where a practice can use or disclose health or genetic information for a 'secondary purpose'. These are:

- Research- if relevant to public health or safety and it is impracticable to obtain a patient's consent. The research must be conducted in accordance with research guidelines and the practice must reasonably believe that the information will not be further disclosed by the recipient.
- Prevention of a serious threat to the life, safety or health of a genetic relative. ***Example:*** *a female daughter may request access to her mother and grandmother's medical records to determine the nature of their disease.*
- Responsible person/Guardian – where a patient is either physically or mentally incapable of giving consent, a practice may disclose information to a responsible person or guardian where the disclosure is necessary to provide appropriate care or treatment to the patient or for 'compassionate reasons'. The disclosure must not be contrary to the wishes of the patient and limited to the extent necessary for care or compassion.

APP 7 Direct Marketing

The practice must not use personal information for direct marketing unless the individual has given specific consent for this to occur.

Direct marketing involves the use of personal information to communicate with an individual to promote goods and services.

Example: *sending patients an SMS offering discounted services at the practice is direct marketing and not permitted.*

Direct marketing is permitted where an individual would have a reasonable expectation that this would occur and they can easily 'opt out'.

APP 8 Cross border disclosure of personal information

If the practice is going to send personal information overseas, it must take reasonable steps to ensure the overseas recipient will not breach the APPs. There are exceptions where the overseas recipient has a similar enforceable law in place or the patient has consented after being expressly informed that information will be sent overseas.

***Example**: having a contract with an overseas cloud service provider that requires compliance with APPs.*

APP 9 Use of Government Identifiers

The practice must not adopt, use of disclose a government related identifier unless:

- the adoption, use or disclosure is required or authorised by law
- it is reasonably necessary to verify the identity of the individual.
- It is reasonably necessary to fulfil the obligations to a Commonwealth agency or state or territory authority;
- The practice believes it is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public;
- The practice reasonably believes use or disclosure is necessary to take action in relation to suspected unlawful activity or misconduct of a serious nature
- The practice reasonably believes use or disclosure is necessary for enforcement related activities of an enforcement body.

A government related identifier includes a Medicare number, Centerlink reference number, driver's licence or passport number.

Example: *the practice is not permitted to use Medicare numbers as the basis for patient identification. However, a practice can view and record Medicare numbers to verify the identification of a patient and for billing purposes.*

APP 10 Quality of personal information

Practices must take reasonable steps to ensure the personal information it collects uses or discloses is accurate, up to date complete and relevant.

APP 11 Security of personal information

Practices must take reasonable steps to protect the personal information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.

***Example:** Practices should issue staff with passwords to access patient databases that are changed on a regular basis, and store hard copy files in lockable filing cabinets or rooms, accessible only to authorised practice staff.*

APP 12 Access to personal information

The practice must, on request, provide a patient with access to their personal information within a reasonable time, unless an exception applies (see APP 6 above).

The practice is entitled to charge a 'reasonable' fee for access under the *Privacy Act 1988* (Cth). The Victorian *Health Records Act* 2001 (Vic) sets specified fees for access to medical records. Further information on these fees can be obtained from AMA Victoria.

Any refusal must be accompanied by written reasons and information on how the patient may lodge a complaint.

APP 13 Correction of personal information

A practice must take reasonable steps to ensure the personal information it holds is up to date, accurate, complete, relevant and not misleading. There is a positive obligation on practices to correct information where it is wrong.

The practice must acknowledge a request for an amendment to their medical records, within a reasonable time. No charge can be made for the practice making the requested changes.

Example: *Reception staff should confirm the contact details of the patient are up to date when they present for an appointment.*

Health Records Act 2008 (Vic) obligations

In addition to the obligations imposed by the APPs under the *Privacy Act 1988* (Cth), the *Health Records Act 2008* (Vic) imposes 11 Health Privacy Principles (HPPs) which apply specifically to the collection, use, disclosure and handling of health information in Victoria.

The HPPs are substantially the same as the APPs and so it is not required to set them out separately. There are, however, two added obligations imposed by the HPPs that are not included in the APPs. These are:

HPP 10 – a practice must provide a patient with information about their medical record if the practice is transferred, sold or closed.

HPP 11 – a practice is required to transfer a patient's health information to another health service provider upon request from the patient.