



**Allied Health
Professions
Australia**

Private Practice Privacy Guide 2020

ahpa.com.au

ABN: 60 083 141 664

Disclaimer: This guide is prepared for general information purposes only. To the best of the Allied Health Professions Australia's (AHPA's) knowledge, this information is valid at the time of publication. AHPA makes no warranty or representation in relation to the content or accuracy of the material in this publication. AHPA expressly disclaims any and all liability (including liability for negligence) in respect of the use of the information provided. AHPA recommends you seek independent professional advice prior to making any decision involving matters outlined in this publication.

Contents

Overview	3
Private practice and the Australian Privacy Principles	4
APP 1 – Open and transparent management of personal information	4
APP 2 – Anonymity and pseudonymity	4
APP 3 – Collection of solicited personal information	5
APP 4 – Dealing with unsolicited personal information	5
APP 5 – Notification of the collection of personal information	5
APP 6 – Use or disclosure of personal information	6
APP 7 – Direct marketing	7
APP 8 – Cross border disclosure of personal information	7
APP 9 – Adoption, use and disclosure of government related identifiers	7
APP 10 – Quality of personal information	8
APP 11 – Security of personal information	8
APP 12 – Access to personal information	8
APP 13 – Correction of personal information	9
Suggestions on developing a Privacy Policy	11
1. Appoint a Privacy Officer	11
2. Learn about the Australian Privacy Principles (APPs)	11
3. Conduct an initial internal privacy audit	11
4. Compare your current practices with requirements of the APPs	11
5. Consult with relevant people to develop the plan	11
6. Develop a complaints handling procedure	11
7. Link your privacy policy with your data breach response plan	11
Next steps once you have developed your Privacy Policy	12
1. Train staff	12
2. Inform your clients about your Privacy Policy and complaints procedure	12
3. Conduct annual privacy audits and review your Privacy Policy	12
Retention of personal information	12
Victorian Legislation	12
NSW Legislation	13
Selling or closing a practice	13
Conclusion	14
Appendices	
Appendix 1: Relevant legislation	15
Appendix 2: Questions to Guide a Self-Audit	16
Appendix 3: Access Checklist	17
Appendix 4: Audit Questions and Breaches Information	18
Privacy Audit Questions	18
Breaches of the APPs	19
Appendix 5: Sample Consent Form	20
Appendix 6: Sample Collection Statement	21

Overview

Privacy of personal information, including health information, is more than a professional and ethical responsibility – it is a legal requirement. In Australia the Privacy Act 1988 (Cth) (**Privacy Act**), regulates the handling of an individual's personal information. The private sector provisions of the Privacy Act apply to all health service providers who hold any health information. For a list of relevant laws refer to Appendix 1. Practitioners employed in the Commonwealth public sector must also comply with the Privacy Act. This privacy guide, however, is concerned only with the private sector provisions of the Privacy Act.

The Privacy Act includes a set of harmonised privacy principles, the Australian Privacy Principles (**APPs**). The APPs replaced the Information Privacy Principles (**IPPs**) and the National Privacy Principles (**NPPs**). Thus, since 12 March 2014 allied health practitioners working in Commonwealth public organisations and private practices will operate under one set of privacy laws: the Australian Privacy Principles. [APPs guidelines](#), as well as resources regarding their application, can be found on the website of the [Office of the Australian Information Commissioner](#).

The intent of this guide is to provide practitioners whose national association is a member of AHPA with information and resources so that they may increase their understanding and knowledge of current privacy legislation and more specifically the APPs. This privacy guide contains sections on the APPs and how they relate to private practice, a step-by-step guide to developing a Privacy Policy, information on how to protect the privacy of clients' personal information when selling or closing a practice and information on retention of personal information; there are also a number of appendices at the end of the guide.

This guide does not reproduce all of the details of the APPs – practitioners can readily obtain these from www.comlaw.gov.au. Instead, the guide focuses on some of the practical applications of the APPs, giving examples and explanations of privacy practices, where appropriate.

The appendices include a range of templates that can be used to create your own documents. Please read this guide carefully and consult other resources where necessary to ensure that you fully appreciate and understand the importance of the privacy legislation in relation to your own particular circumstances before adapting these documents for your use.

It should be noted that this guide is prepared for general information purposes only – it does not exhaustively cover all issues regarding the Privacy Act, the APPs or privacy generally. The guide is not addressed to any specific health profession and it may not cover all issues relevant to each health profession. Further, this document does not constitute and should not be relied upon for legal advice. Each practitioner has an independent obligation to ascertain the legal requirements concerning privacy and health records that affect them and to comply with those requirements. Practitioners working in the State/Territory public sector may find the guide of interest; however, they would also need to have regard to their employing organisation's privacy policies and procedures and any additional, applicable State or Territory legal requirements.

Further, practitioners should be aware that they may be subject to further, specific legal, regulatory professional or ethical requirements concerning their use and management of personal and health information in their profession or practice.

Private practice and the Australian Privacy Principles (APPs)

This section of the guide covers how the APPs relate to the specific circumstances of private practice. Some areas may require practitioners to adopt numerous changes to the way they manage clinical records, while other areas may already be reflected in practitioners' current processes as they may overlap with a practitioner's professional obligations and those prescribed by their relevant association's or board's code of ethics and professional standards.

A summary of the APPs is set out below.

APP 1 - Open and transparent management of personal information

A practitioner must take reasonable steps to implement practices, procedures and systems relating to their functions and activities that:

- » will ensure that they comply with the APPs; and
- » will enable them to deal with inquiries or complaints from individuals about their compliance with the APPs.

A practitioner must have a clearly expressed and up-to-date Privacy Policy about their management of personal information. On request, all clients and other individuals must be provided with a copy of the Privacy Policy. The policy may not need to be excessively long or detailed – however, it needs to include enough information to ensure it complies with the Privacy Act. It can be made available in a number of ways – as a sign in the practice or in a handout or brochure or on a practitioner's or practice's website.

The minimum information that a Privacy Policy must contain includes:

- » The kinds of personal information the practitioner collects and holds.
- » How the practitioner collects and holds personal information.
- » The purpose for which the practitioner collects, holds, uses and discloses personal information.
- » The parties to whom personal information is disclosed.
- » How an individual may access personal information about the individual that is held by the practitioner and seek the correction of such information.
- » How an individual may complain about a breach of the Australian Privacy Principles and how the practitioner will deal with such a complaint.
- » Whether the practitioner is likely to disclose personal information to overseas recipients.
- » If the practitioner 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.

Please note: there may be clients who may not fully understand this written information, or may need assistance to do so. In such cases, the provision of the information may need to involve qualified interpreters or other appropriate persons or professionals/specialists who can ensure that the message is conveyed and fully understood. Furthermore, it is preferable for written information to be provided in plain English.

The following section titled "How to Develop a Privacy Policy" lists some suggested steps you can undertake to develop a Privacy Policy.

APP 2 - Anonymity and pseudonymity

The principle of anonymity and pseudonymity revolves around the fact that a client may choose to attend your clinic anonymously or under the name of an alias. This is possible and is permitted where it is lawful and practicable. However, this is unlikely to occur within the context of most health practices or health consultations, as most clients accessing treatment need to identify themselves appropriately to receive appropriate care and

to be able to claim rebates from third party funders such as private health funds, Medicare, DVA, transport and accident or worker's compensation authorities etc. It will also generally be necessary for clients to properly identify themselves to ensure appropriate records are kept and for continuity of care to be provided.

APP 3 - Collection of solicited personal information

The collection of solicited information may occur in many forms, some of which might not be immediately apparent. The most obvious method is collecting information directly from an individual – for example, through a form or during a consultation. Other methods include letters and reports received from external sources, either through your request or otherwise, as well as daily practices where information is collected from the patient in the circumstances of general clinical practice (i.e. name, address, phone number, case history etc.). Any notes taken during treatment sessions are also deemed as “collected information”, in addition to general and clinical details that are recorded during an assessment. An opinion or interpretation of what is said or read is also considered “information collected” if it is written down and kept. This information may be in hard copy, electronic, video or audio (both analogue and digital) formats.

APP 3 provides that only information that is reasonably necessary for, or directly related to, one or more of an entity's functions or activities should be collected and it should be collected by lawful and fair means. Generally, a health practitioner will need to collect and record information that is necessary and relevant to the care (assessment or treatment) provided to the client.

In some circumstances, you may need the consent of the client to collect their information. Consent may be express or implied and it may be given verbally or in writing. The process of obtaining consent needs to be conducted in a manner that results in the client actually understanding what they are consenting to, not just have gone through a process of information provision. This process may be aided if the provision of information occurs in a conversational manner, rather than rote reading through a standard script. In some circumstances, it may be necessary to use a qualified interpreter. If a client lacks the capacity to provide informed consent in relation to a matter concerning their information, it may necessary to seek such consent from a surrogate decision maker who has authority to provide consent on behalf of that client.

The location of the collection of the information also needs to be considered. For example, speaking to a client in a waiting room or in an inadequately sound proofed office may result in a breach of privacy if another person overhears that conversation.

APP 3 permits the collection of a client's health information in certain circumstances without the requirement to obtain their consent – for example, where the collection is necessary for the provision of a health service to the client. For a complete list of the circumstances where collection is permitted without the requirement for consent, you should refer to APP 3.

APP 4 - Dealing with unsolicited personal information

Occasionally, a practitioner will receive personal information about a client which they have not sought – this is deemed unsolicited personal information. If a practitioner receives personal information and the practitioner did not solicit that information, the practitioner should determine whether he or she could have collected the information under APP 3 if they had solicited that information.

If the practitioner determines that he or she could not have collected the personal information under APP 3, the practitioner must destroy the information or ensure that the information is de-identified, provided it is lawful and reasonable to do so.

If the practitioner determines that he or she could have collected the personal information under APP 3, he or she must treat the information in accordance with APPs 5 to 13 as if he or she had collected the information under APP 3.

APP 5 - Notification of the collection of personal information

At or before the time a practitioner collects personal information about an individual, the practitioner must take reasonable steps to notify or make the individual aware of the following matters:

- » the identity and contact details of the practitioner or practice;

- » if the practitioner or practice collects the personal information from someone other than the individual;
- » if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order;
- » the purposes for which the practitioner collects the personal information;
- » the main consequences (if any) for the individual if all or some of the personal information is not collected – this will usually be that the practitioner may be unable to provide any or certain services to the client;
- » any other person or body to which the practitioner usually discloses personal information of the kind collected;
- » that the practitioner’s or the practice’s Privacy Policy contains information about how the individual may access the personal information about the individual that is held and seek the correction of such information;
- » that the practitioner’s or the practice’s Privacy Policy contains information about how the individual may complain about a breach of the APPs and how the practitioner or the practice will deal with such a complaint;
- » whether the practitioner is likely to disclose the personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

The above information is usually contained in a document often referred to as a ‘collection statement’ - see Appendix 7 for an example of a collection statement. Many organisations incorporate these details into their privacy policy and provide a copy of their privacy policy to individuals at the relevant time.

APP 6 - Use or disclosure of personal information

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

- » the individual has consented to the use or disclosure of the information; or
- » one of the circumstances set out in APP 6.2 or 6.3 applies in relation to the use or disclosure of the information.

The “use” of information refers to the handling of the information within the practice, while the “disclosure” of information refers to the transfer of information outside the practice.

“Use” of information within a practice for the purpose of providing a health service is the primary purpose of its collection; it is also generally expected by clients as being a part of the delivery of their treatment. It is important that clients are aware of this process. This needs to be made very clear in the event that another practitioner may review or take over the delivery of care within the practice. In relation to adequate continuity of care for clients and their personal information, it is good practice to inform clients that their personal information may be accessed and transferred between clinicians and/or other professionals. APP 6 also permits a number of uses without the requirement to obtain the client’s consent for that use. The most common example would be the use of personal information for a purpose related to providing a health service to the client.

“Disclosure” is also often expected and considered to be an important part of the effective management of clients’ information. Examples of disclosures include reporting to teachers, doctors, specialists, carers or other health professionals. A disclosure which occurs in relation to the primary purpose of collection is permitted. However, having clients specify permission to supply information to another party may be an effective way of ensuring that they are aware of who and how information is being disclosed and for what purposes (preferably in writing; or documenting in the client’s file that permission was obtained for disclosure of information to other clinicians/ health professionals).

Practitioners should already be following good practice regarding the gaining of consent to use and disclose information as part of professional standards. A Privacy Audit will provide the opportunity for you to ensure that there is consistency in your particular practice.

APP 6.2 sets out a number of circumstances where personal information may be lawfully used or disclosed in circumstances other than for the primary purpose of collection. These include:

- » where the use or disclosure of the information is required or authorised by or under an Australian law or a

court/tribunal order - for example, in most jurisdictions there is the mandatory reporting of possible child abuse to authorities.

- » where there is a 'permitted health situation', as defined in the Privacy Act. This includes use or disclosure for the purpose of providing a health service and for research. In the case of using or disclosing the information for research, certain additional conditions need to be met. Further, it may also be permissible in some circumstances to disclose an individual's genetic information to a genetic relative, provided the conditions set out in the Privacy Act are met.
- » Where there is a 'permitted general situation', as defined in the Privacy Act. This includes use or disclosure to protect the health and safety of the client or the public at large.

The circumstances of each case need to be considered. For example, in the event of an immediate or impending act of assault or involving a weapon, public safety may override the risk of a breach. When unsure, you should seek legal advice.

For a complete list of the permitted uses and disclosures, you should refer to APP 6.

As a general rule, you should not use or disclose a client's personal information in a manner that goes against their expressed wishes or instructions. However, there are exceptions to this rule – for example, concerns regarding the health and safety of the client or another person may in certain circumstances be sufficient to justify disclosure. Again, in cases of doubt, you should seek legal advice.

APP 7 - Direct marketing

Generally, a practitioner must not use or disclose an individual's personal information for the purpose of direct marketing. To do so may not only be a breach of the Privacy Act, but may also be unethical and unprofessional and breach your profession's or association's rules of conduct and ethical standards; it could potentially even harm your relationship with a client.

APP 7 provides that personal information may be used for direct marketing purposes in the following circumstances:

- » the practitioner collected the information from the individual, the individual would reasonably expect the practitioner to use or disclose the information for that purpose and the practitioner provides a simple means by which the individual may easily request not to receive direct marketing communications; or
- » the individual has consented to the use or disclosure of the information for that purpose, the practitioner provides a simple means by which the individual may easily request not to receive direct marketing communications, and in each direct marketing communication with the individual, the practitioner includes a prominent statement that the individual may make such a request.

As soon as a person makes a request not to receive direct marketing material, the practitioner must comply with that request.

Even if the Privacy Act permits the use and disclosure of an individual's personal information for direct marketing, a practitioner should exercise caution before doing so as this may constitute a breach of their relevant profession's code of ethics or constitute professional misconduct for that profession.

APP 8 - Cross-border disclosure of personal information

The Privacy Act imposes specific rules regarding the transfer or disclosure of personal information to a person who is overseas. APP 8 impose restrictions on the transfer of personal information to overseas recipients because once the information leaves Australia, it will no longer have the protections afforded by the Privacy Act.

A practitioner who intends to disclose personal information to an overseas recipient should carefully consider the requirements of APP 8.

APP 9 - Adoption, use or disclosure of government related identifiers

Many practices allocate a client number to each client for ease of identification. APP 9 states that such identifier

cannot be one that is already assigned by a Commonwealth Government Authority. Therefore, identifiers such as Tax File Numbers, Medicare Numbers or DVA numbers cannot be adopted by a practitioner or practice as their own identifier of a person, unless one of the exemptions set out in APP 9 applies. Exemptions that might apply include:

- » the use or disclosure of the identifier is reasonably necessary for the practice or practitioner to verify the identity of the individual for the purposes of the practice's or practitioner's activities or functions; and
- » the use or disclosure of the identifier is reasonably necessary for the practice or practitioner to fulfil their obligations to an agency or a State or Territory authority – for example, if a client's Medicare number is used for Medicare billing purposes.

APP 10 - Quality of personal information

You must ensure that the information collected is accurate, complete and up-to-date. One way to do this is by ensuring you update a client's details when notified by them of any changes. Also, you must take reasonable steps to ensure that the personal information that you use or disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

APP 11 - Security of personal information

APP 11 requires any person who holds personal information to take reasonable steps to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure.

The possibility of unauthorised access, modification or disclosure of client information needs to be considered. Be aware that there may be others in your practice - for example, cleaners, other clients, students, etc. - who may potentially have access to client files or an individual's personal information. It is critical that you have good procedures, practices and policies in place to guard against unauthorised access and that all your staff are trained in these. You need to actively guard against misuse or loss of information.

Carrying client notes or files around in the car or at home are areas of risk. The Privacy Act doesn't prevent you from taking client notes home or on hospital or other visits, but you would have an obligation to take reasonable steps to secure them when doing so. Other activities that may present a privacy risk include photocopying of client records (for example, if photocopied notes are inadvertently left behind on a photocopier) and the offsite storage of client files. The practice of leaving notes/files on reception counters of waiting rooms or in treatment rooms when the practitioner moves to another task is strongly discouraged. Taking home a laptop computer with client information on it may cause a problem if your car or house is broken into or your car is stolen. Amongst other things, password controls are essential in securing electronic information.

It is important to ensure that information that is no longer needed for any purpose is destroyed or de-identified properly. This is always subject to any other legal requirements or any professional requirements concerning the retention of that information. Securing records to prevent loss due to fire or water also needs to be considered. The above principles apply to all forms of information held in whatever format, such as paper, electronic, video and audio.

APP 12 - Access to personal information

The Privacy Act provides clients with the right to access their personal information. This applies to information that has been collected after the 21 December 2001 and to any information collected before that date that is still currently in use. Thus, a client who commenced before 21 December 2001 but is still receiving care or assistance, has the right to access all their personal information held by your practice. A person has the right to seek access only to his/her own records.

APP 12.3 sets out a number of circumstances where access to a client's personal information or records may be denied. One exception to giving access is if you reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

The intent of the Privacy Act is that individuals should have access to their personal information. Upon receiving a request for access, a practitioner must carefully review the client's record to consider whether any APP 12.3 exception to access might apply to any part of the client's record. If access is denied, the practitioner must provide reasons to the applicant for the denial.

There are a variety of ways that the client can access their records – the most common way is by providing a copy of the record to the client. You must provide access by the method nominated by the client. One method is to sit with the client, go through the information with them so that terms and the relevance of notations can be explained.

Requests for access to personal information can be made both orally and in writing. If requests are complex, it may be useful to have clients put it in writing so that the request can be kept on file.

Electronic or hard copies can be provided or you may wish to offer your client a written summary of the information if they agree to this.

The Privacy Act provides that you may charge an individual for giving access to their personal information but you may not charge them for making the request. The charge for giving access – for example, in relation to photocopying charges – must not be excessive.

APP 13 - Correction of personal information

A client has a right to request correction of their personal information if the information is inaccurate, out of date, incomplete, irrelevant or misleading. A practitioner must then take such steps (if any) as are reasonable in the circumstances to correct the 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.

A practitioner should also independently make such correction if he or she believes that the information they hold is inaccurate, out of date, incomplete, irrelevant or misleading, even if a client has not made a request for correction.

If a practitioner refuses to correct the personal information as requested by the individual – for example, because the practitioner believes the information is accurate and complete - the practitioner must give the individual a written notice that sets out the reasons for the refusal and the mechanisms available to complain about the refusal.

When a request for correction is related to assessment outcomes or opinions, the practitioner should not erase the old information if they believe it to be correct. They may however attach a statement detailing the client's perspective/interpretation to the report.

A practitioner must not charge an individual for making a request for correction or for correcting their information.

Notifiable Data Breaches

The Privacy Act requires any organisation which is subject to that Act to notify an affected individual and the Office of the Australian Information Commissioner (**OAIC**) about certain data breaches (**notifiable data breach**) which occur on or after 22 February 2018.

What is a notifiable data breach?

A data breach is a notifiable data breach if:

- » there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation holds;
- » this is likely to result in serious harm to one or more individuals; and
- » the organisation has been unable to prevent the likely risk of serious harm with remedial action.
- » Examples of data breaches in the health care setting include the following:
 - » A system, data, document, material or a device containing personal information is lost or stolen.
 - » A system, data, document, material or a device containing personal information is accessed by a person who does not have authority to access it.
 - » A practice's records or systems containing personal information are hacked by an external person or entity.

- » A practitioner or member of the practice's staff provides or discloses personal information to a person who should not have received it– for example, a file, email or letter containing personal information is sent to the wrong recipient.

What you need to do if a notifiable data breach occurs

If a notifiable breach has occurred, you must report the details of the breach to any individual affected by it and to the OAIC. The notification must include the following information:

- » the identity and contact details of the practice;
- » a description of the data breach;
- » the type of information involved in the data breach; and
- » recommendations about the steps that the individual should take in response to the data breach.

A practice or practitioner must conduct an assessment of a data breach to determine if it meets the above criteria. While the presence of 'serious harm' is a key consideration, it is not defined in the Privacy Act. However, it would include serious physical, psychological, emotional, financial, or reputational harm. Further, steps should be taken to prevent any further harm or damage.

Data breach plan

Practices/practitioners should develop and implement a data breach response plan. A data breach response plan is a framework which sets out the roles and responsibilities involved in managing a data breach and the steps that should be taken if a data breach occurs.

Amongst other things, a data breach response plan will assist a practice/practitioner to:

- » meet their obligations under the Privacy Act regarding taking reasonable steps to protect the personal information held;
- » respond to a data breach quickly and decrease its potential consequences;
- » minimise reputational harm; and
- » preserve trust and confidence.

A data breach response plan should be tailored to the operational structure and requirements of a practice.

Suggestions on developing a Privacy Policy

All health service providers regardless of whether they work as a sole practitioner, they employ a small number of staff or they are a large multidisciplinary organisation are required to develop a Privacy Policy. The level of detail contained in the Privacy Policy will depend on factors including:

- » the size of the practice,
- » the nature of the information collected, used and disclosed,
- » how the practice stores and secures the information, and
- » whether personal information is transferred interstate or overseas.

When developing a Privacy Policy the following steps may be useful:

1. Appoint a Privacy Officer

This is important particularly if there is more than one practitioner/staff member/contractor dealing with client information. The Privacy Officer is the first point of contact when privacy issues arise either internally or from external sources.

2. Learn about the Australian Privacy Principles (APPs)

The APPs principles are a legally binding set of rules.. Practitioners must have an intimate knowledge of the APPs and understand how they apply to their practice.

3. Conduct an internal privacy audit

This is a useful way of working out what sort of personal information the practice collects, holds, uses and discloses and how it does those things. Understanding this is an important step to developing a sound privacy plan. Appendix 1 provides an example list of self-audit questions.

4. Compare your current practices with the requirements of the APPs

Once you have conducted a privacy audit you will also need to consider each of the APPs and consider how each of the principles is currently being handled within your practice. How do your processes measure up and what modifications need to be made? If there are any gaps it is important to consider requesting professional assistance to deal with these key areas of practice (i.e., consultation with a legal representative).

5. Consult with relevant people to develop the plan

Discuss with internal stakeholders (i.e. staff and contractors) and external stakeholders (i.e. clients and other service providers) their expectations and thoughts regarding current practices. External advice is also a good way of objectively testing whether or not you are meeting the requirements of the privacy legislation. More information can be obtained from the website of the Office of the Australian Information Commissioner: www.oaic.gov.au and there are lawyers who have expertise in the area of privacy law.

6. Develop a complaints handling procedure

This will ensure that any complaints are handled immediately and effectively. It is an important part of managing privacy issues within the practice.

7. Link your privacy policy with your data breach response plan

A practice's or practitioner's privacy policy and data breach response plan support and complement each other.

Next steps once you have developed your Privacy Policy

1. Train staff

Once the privacy procedures and practices have been decided, it is critical that all staff within the practice follow this process to ensure that the information is managed, understood and kept secure. Induction of new staff and training and regular retraining of existing staff is paramount to ensuring that all staff members (including support staff) have the necessary knowledge and skills to be able to follow privacy policies and procedures in your practice.

2. Inform your clients about your Privacy Policy and complaints procedure

The Privacy Act stipulates that on request clients should be provided with a copy of the health provider's Privacy Policy. AHPA believes it is good practice to provide to each client or display in your practice a copy of your Privacy Policy and complaints procedure.

3. Conduct annual privacy audits and review your Privacy Policy

It is good practice for practitioners to at least annually but more frequently if required, conduct privacy audits, review their Privacy Policy and retrain staff.

Retention of Personal Information

APP 11 provides that a practice or practitioner must destroy or de-identify personal information which is no longer required, unless otherwise required to retain it by law. This requirement must be considered in conjunction with the retention requirements of other Commonwealth laws and any applicable State/Territory laws.

The Privacy Act is intended to operate in conjunction with State and Territory based legislation regarding the retention of health records. Victoria and New South Wales are two States which have legislated the retention of personal information in the private sector.

Victorian Legislation

Under the Health Records Act 2001 (VIC), a legislative requirement exists which specifically refers to the retention of health information by all health service providers in both the public and private sectors. Health Privacy Principle 4.2 of the Health Records Act 2001 (VIC) states:

“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, authorized or required by the regulation 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.”

New South Wales Legislation

The *Health Records and Information Privacy Act 2002* (NSW) provides for the retention of health information under Division 2 of the Act. It states the following:

- “(1) A private sector person who is a health service provider must retain health information relating to an individual as follows:
- (a) in the case of health information collected while the individual was an adult—for 7 years from the last occasion on which a health service was provided to the individual by the health service provider;
 - (b) in the case of health information collected while the individual was under the age of 18 years—until the individual has attained the age of 25 years;
- (2) A health service provider who deletes or disposes of health information must keep a record 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 or disposed of;
- (3) A health service provider who transfers health information to another organisation and does not continue to hold a record of that information must keep a record of the name and address of the organisation to whom or to which it was transferred;
- (4) A record referred to in subsection (2) or (3) may be kept in electronic form, but only if it is capable of being printed on paper;
- (5) Nothing in this section authorises a health service provider to delete, dispose of or transfer health information in contravention of an Act (including an Act of the Commonwealth) or any other law.”

Practitioners must carefully consider the requirements of the Privacy Act, any relevant State or Territory legislation, any requirement imposed by their professional regulatory body or association and any other requirement that is relevant to the retention of records (for example, a requirement imposed by their professional indemnity insurer) in developing and implementing a document retention or destruction policy.

Selling or Closing a Practice

There is no Australian Privacy Principle that specifically deals with the transfer or closure of a health service provider’s practice. The overall framework of obligations set out in the APPs requires appropriate information handling in such circumstances. The principles which may be relevant include those that relate to collection, use and disclosure and data security.

However, the *Victorian Health Records Act 2001* contains a specific health privacy principle concerning the transfer or closure of a health service provider’s practice. Victorian practitioners are required to comply with the specific requirements of this privacy principle (Health Privacy Principle 10).

The following is a summary of some recommended guidelines that may be useful for members to consider in the event of the sale or closure of their practice.

A practice may cease to operate due to retirement, sale, amalgamation, or the death of a practitioner. It is the responsibility of the incumbent practitioner to have a plan in place for the way in which records will be handled in the event of any of these circumstances.

Where clients can be contacted, they should be notified of the forthcoming transfer or closure of a practice and asked to nominate (preferably in writing) another service provider to whom their files should be transferred.

Where clients cannot be contacted, the practitioner will have to consider whether it is appropriate to transfer the files or store the files of each current and non-current client.

The choices available to the provider include transferring, retaining or handing the information to the individual. One or more of the following steps may form part of the transfer process:

1. Publish a notice in the newspaper circulating in the local area, setting out the details of the proposed sale, transfer or closure and stating whether the health information is to be kept by the provider, is to be made available to the client or will be transferred to another provider.
2. Place a notice at the business or practice in clear view for a reasonable period prior to the date of the sale, transfer or closure.
3. Notify (in writing) each client currently receiving a program/treatment or whose condition is scheduled to be monitored or reviewed by the departing practitioner, about the changes to the practice, where it is practicable to do so.

These steps are suggested as actions that may assist the transfer process. However, it is important for each practitioner to check whether there are any legal requirements in the State or Territory in which they practise that may impact on the actions that need to be taken. Further, practitioners may also have other obligations that are relevant in these circumstances – for example, those specified by their professional regulatory body or professional association or professional indemnity insurers.

Care should always be taken before transferring or destroying records. The transferring or destroying of records must be carried out with extreme care and in compliance with all applicable laws. Generally, any destruction of client records should be made in a secure manner that preserves the confidentiality and privacy of the records throughout the destruction process. In addition, practitioners should take into account their own State/Territory's requirements with respect to the retention of records (refer to Appendix 8 – Retention of Records).

Conclusion

A health service practitioner in private practice has a legal obligation to comply with the Australian Privacy Principles. It is important for practitioners to ensure that their privacy policies, procedures and practices comply with the 13 Australian Privacy Principles and the Privacy Act generally. Further, practitioners should ensure that staff within their practice also understand and comply with these obligations. Practitioners should generate their own document(s) and processes within the context in which they practice and make sure that their clients are adequately informed about their privacy practices. It is also worthwhile for practitioners to have their legal representative review their privacy procedures and policies to ensure they comply with the Privacy Act.

Appendix 1: Relevant legislation

Practitioners must generally comply with the following laws and requirements relating to privacy and health records:

- » the *Privacy Act 1988* (Commonwealth),
- » their respective State/Territory's legislation (see below), and
- » any reasonable recommendation, guideline or policy set down by the Australian Information Commissioner.

Examples of relevant State/Territory legislation includes:

- » *Privacy and Data Protection Act 2014* (VIC), (this is generally relevant for practitioners working in the Victorian public sector)
- » *Health Records Act 2001* (VIC),
- » *State Records Act 1998* (NSW),
- » *Health Records and Information Privacy Act 2002* (NSW), and
- » *Health Records (Privacy and Access) Act 1997* (ACT).

NOTE: The above list regarding the States and Territories is not exhaustive and may change. AHPA members should ensure that

Appendix 2: Questions to Guide a Self-Audit

1. What personal information does the practitioner/practice collect? Is any of the information sensitive information?
2. How does the practitioner/practice collect this information? Common ways include during a consultation, standard forms or client surveys.
3. Where and how does the practitioner/practice store this information? It may be kept in a single database or it may be in several locations.
4. Who within the practice has access to the personal information held and who actually needs to have access to the information?
5. Does the practice have measures to protect the personal information it holds from unauthorized access?
6. Why does the practitioner/practice collect the personal information it collects? Is it needed for a particular function or activity?
7. Would your clients know that you are collecting the information?
8. How does the practitioner/practice use or disclose the information?
9. Does the practitioner/practice give the information to anyone outside the practice and for what purpose?
10. Does the practitioner/practice contract out any functions or activities involving personal information? What measures are taken to protect this information?
11. Does the practitioner/practice make individuals aware of the practice's intended uses and disclosures of that information?
12. Is relevant personal information accurate, complete and up-to-date?
13. Does the practitioner/practice transfer any personal information overseas? If so, to whom, and in which countries do such persons reside?
14. Does the practice have a data breach response plan?

Appendix 3: Access Checklist

Make sure that you are familiar with the Privacy Act and the APPs before administering this checklist to ensure that you are using this information within the context of the Privacy Legislation.

1. Are your clients aware from the outset of their rights to access their information?
2. How would you or your staff process a request if a client requests access to their information?
3. Do you have a procedure in place to be able to respond to this request?
4. Do you have a designated privacy officer if there is more than one person within the practice?
5. Are all staff aware of the procedures to be followed?
6. Will accessing information incur a cost to your client?
NB: Remembering that you cannot charge a person for making a request and any charges imposed for giving access to the information must be reasonable.
7. Is the client being encouraged to be specific about which aspect, assessment or dates they want information on? This will then limit time, expense and potential confusion for all concerned.
8. If all the information on a client's file is being requested, how will you facilitate this?
9. Is the client happy to sit in a room and read the information or would they like a copy of the information? If they choose to sit and read it then it may be necessary for someone be with them to ensure client wellbeing.
NB: It is the intention of the Privacy Act to allow clients easy access to their information for no or low cost.
10. Does the client know an estimated cost prior to you commencing any photocopying of information?
11. Does the client want the practitioner to explain the information contained in the records? If so any fee charged to do this must be reasonable.
12. Would writing a summary report satisfy the requests of the client? Again, any fee charged must be reasonable.
13. Is the request in writing? They do not need to be, however, if the request is complex, then requesting this may be the most effective way of being clear about what is being requested.
14. Has the request been made by a third party and if so has the client given their permission, or is that person entitled to be requesting that information? For example: in a custody issue or power of attorney context? It is recommended that you seek specific legal advice if you are at all in doubt about whether to grant access to a third party.

Appendix 4: Audit Questions and Breaches Information

Here are a series of questions you may like to ask when conducting a privacy audit and what to consider if there is a breach of the APPs. This audit is based on the principles of the APPs so it is important for you to know and understand the APPs before conducting the audit.

Privacy Audit Questions

1. Information Collected

Is the collection fair, lawful and non-intrusive. Do you properly inform individuals of the name of the person/organisation that is collecting the information?

2. Right of Access

Is the client aware that they can access their information if they choose to and how to go about doing that?

3. Use & Disclosure

Is the information that you are collecting going to contribute to the quality of the service that you deliver and how? Only collect what is really needed to ensure the quality of service delivery. Have you explained the purpose of the collection and the usual disclosures?

4. Secondary uses of information

Do you have informed consent of the client, guardian or power of attorney to be releasing information for a secondary use? If it is directly related and would be reasonably expected then consent is not required. However it would be recommended to always have the client, guardian or power of attorney (as the case may be) well informed about the circumstances of disclosure.

5. Legal requirement for the collection of some information

There may be some instances where it is required by law to collect particular information. If so, then it is useful for the practitioner to know when they are doing this and for what reason, under which law and why.

6. Data Quality

How accurate is the information being collected, how complete is the information and how up-to-date is the information? What mechanisms do you have in place for routinely updating or checking this information?

7. Data Security

Who has access to the information? Is it the appropriate people only (who have a legitimate reason to access information) and how do they have access to it? Do they have access electronically or in hard copy form? Is the information safe from misuse? (e-copy, hard copy, audio or video information)

8. Openness

How accessible is your privacy policy and where is your privacy statement displayed?

9. Access and Correction

What procedures do you have in place for requests for information? Are all staff familiar and trained in the procedures of how to respond to requests for information?

10. Identifiers

Are you using your own identifiers on files and not Commonwealth Government identifiers to identify clients? (For example, DVA, Tax File, Medicare etc.)

11. Anonymity

Do you maintain the clients' anonymity wherever possible, in all conversations in all contexts wherever possible?

12. Transborder Dataflow

Are you ever requested to send personal information overseas? You may only send personal information overseas in the circumstances prescribed in the Privacy Act. You may send non-identifying information overseas without the consent of the individual.

13. Sensitive Information

Do you collect sensitive information? Do you have a lawful permission to collect that sensitive information?

14. Data breach

Do you have a data breach response plan? Do your staff understand how to manage a data breach?

Breaches of the APPs

Individuals are within their rights under the Privacy Act to direct privacy related complaints to the organisation concerned. Where possible you should attempt to rectify the problem and satisfy the complainant's request. Have a procedure in place and ensure that all staff are well trained to facilitate this process. Ensure that all new staff are well trained in the policy and procedures that you adopt for your practice.

If the complainant is not happy with the response then they may take their complaint to the Office of the Australian Information Commissioner. If the complaint is upheld by the Office of the Australian Information Commissioner, the possible outcomes include: an apology, a change to the respondent's practices or procedures, staff training, or compensation for financial or non-financial loss.

Appendix 5: Sample Consent Form (regarding privacy)

A sample consent form (regarding privacy) is provided below. It is of a general nature only and may not address or be relevant to your circumstances or requirements. You should develop a working knowledge of the Australian Privacy Principles before developing your consent form. Practitioners will need to consider whether it is appropriate for them to use such a consent form and in what circumstances they may use it.



**Allied Health
Professions
Australia**

(Name of Organisation/Practice) needs to collect information about you for the primary purpose of providing a health service to you. In order to thoroughly assess, diagnose and provide health care, we need to collect some personal information from you. If you do not provide this information; we may be unable to provide some or all of our services to you. Your information will also be used for:

- a. The administrative purpose of running the practice;
- b. Billing either directly or through an insurer or compensation agency;
- c. Use within the practice if discussing or passing your case to another practitioner within the practice for your ongoing management;
- d. Disclosure of information to your doctors, other health professionals or to teachers to facilitate communication and best possible care for you; and
- e. In the case of insurance or compensation claim it may be necessary to disclose and/or collect information that concerns your return to work to an insurer or your employer.

We do not disclose your personal information to overseas recipients.

(Name of Organisation/Practice) has a Privacy Policy that is available on request and is available in the waiting area. That policy provides guidelines on the collection, use, disclosure and security of your information. The Privacy Policy contains information on how you may request access to, and correction of, your personal information and how you may complain about a breach of your privacy and how we will deal with such a complaint.

To ensure the process of quality treatment provision, information about your assessment results and progress may be given to relevant other service providers, who are involved in your management. These may include your doctor, teachers, specialists, insurers, solicitors or employers.

I, (Name), have read the above information and understand the reasons for the collection of my personal information and the ways in which the information may be used and disclosed and I agree to that use and disclosure.

I understand that it is my choice as to what information I provide and that withholding or falsifying information might act against the best interests of my assessment and therapy progress.

I am aware that I can access my personal and health information on request and if necessary, correct information that I believe to be inaccurate.

I understand that if access is denied I will be informed of the reasons for this.

I have been provided with or have been given an opportunity to obtain a copy of (Name of Organisation/ Practice) privacy policy.

SignedDate

ahpa.com.au ABN: 60 083 141 664

Appendix 6: Sample Collection Statement

A sample collection statement is provided below. It is of a general nature only and may not address or be relevant to your circumstances or requirements. The text below provides examples of some of the matters a collection statement should include. Please note this is not intended to be a Privacy Policy but instead it is a collection statement as outlined in APP5. This statement contains most of the details that might be contained in a privacy policy and you should think about whether simply having a privacy policy that contains all relevant information (and that could also be used as a collection statement) would be sufficient for your requirements. You may choose to provide this information attached to a consent form or in a brochure or displayed as a poster in your practice. You need to be familiar with the material in this Privacy Guide and have a working knowledge of the Australian Privacy Principles before developing your privacy statement. You may adapt the statement to meet your individual needs. This statement needs to be provided before or at the time of collection of information and you must ensure that your clients have fully understood the purposes of collecting the information. The statement that you develop must obviously be consistent with your privacy policy.



Personal and Health Information Collection Statement

(Name of the practice) is an independent practice under the ownership of (name of the company, partnership or sole trader)

You may contact (name of practice) by writing to (name of practice & address), by emailing (insert email address) or by calling (name of the Privacy Officer).

Our Privacy Policy (available upon request) contains information on how you may request access to, and correction of, your personal information and how you may complain about a breach of your privacy and how we will deal with such a complaint.

(Name of practice) needs to collect information about you for the primary purpose of providing care and treatment. In order to fully assess, diagnose and treat you, we need to collect some personal information from you. This information will also be used for the administrative purposes of running the practice such as billing you or through an insurer or compensation agency. Information will be used within the practice for handover if another practitioner provides you with assistance.

(Name of practice) may disclose information regarding diagnosis or treatment to your Doctor or other treatment providers if necessary for your care or otherwise with your consent. In the case of insurance or compensation claims, it may be necessary to disclose information and/or collect information that affects your treatment and return to work. (Name of Practice) will not disclose your information to commercial companies, however specific service or product information as deemed suitable for your management, may be forwarded to you by us, unless you instruct (name of practice) not to forward this type of information. Your written consent will be obtained at the start of your treatment in order to carry out the above activities. We do not disclose your personal information to overseas recipients.

Information at (name of practice) is stored securely and only practice staff has access to it. (Name of practice) takes all reasonable steps to ensure that information collected about you is accurate, complete and up-to-date. You may request access to your information. You may also request correction of your information if you believe that any of the information is inaccurate. If you do not provide relevant personal or health information, in part or in full, to (name of practice) we may be unable to provide some or all of our services to you. This may impact the care we are able to provide to you. Any concerns that you may have about this statement or about your management can be directed to (name of privacy/complaints officer & the address, phone number).

ahpa.com.au ABN: 60 083 141 664