Australian Traditional-Medicine Society Ltd

ATMS

THE PRIVACY ACT AND THE AUSTRALIAN PRIVACY PRINCIPLES

FREQUENTLY ASKED QUESTIONS

CONTENTS

How is Privacy governed in Australia?

The *Privacy Act 1988 (*Cth) (**the Privacy Act**) outlines how individual's personal information (which includes sensitive and health information) can be collected, handled, stored, disclosed and used by companies, business' and organisations. Most of this information is outlined in the 13 Australian Privacy Principles (**APP's**).

In some states and territories additional legislation may exist which governs how to deal with personal information and the privacy of clients and patients. This legislation may include but is not limited to:

Commonwealth	*Spam Act 2003* (Cth)
Victoria	*Information Privacy Act 2000* (VIC) *Victorian Health Records Act 2001* (VIC)
New South Wales	*Privacy and Personal Information Protection Act 1998* (NSW) *Health Records and Information Privacy Act 2002* (NSW)
Queensland	*Information Privacy Act 2009* (QLD)
Tasmania	*Personal Information and Protection Act 2004* (TAS)
South Australia	Code of Fair Information Practice No specific legislation
Western Australia	No specific legislation
Australian Capital Territory	No specific legislation
Northern Territory	*Information Act 2002* (NT)

Practitioners and health care providers may have obligations under the above legislation, in addition to their obligations under the Privacy Act and the APP's.

Does the Privacy Act apply to me?

The Privacy Act and APP's apply to businesses or organisations with an annual turnover of $3million or more. However, if entities collect health information about individuals they are also covered by the Privacy Act and the APP's regardless of their annual turnover.

For this reason, health care providers and practitioners are required to comply with the obligations set out in the Privacy Act and APP's. Please contact the ATMS or the Office of the Australian Information Commissioner if you are unsure of this.

- ***I have been told that my State/Territory does not have any specific Privacy legislation for private health care providers. Does this mean I am not bound by any privacy legislation?***

No. The Federal Government Privacy Act, the *Privacy Amendment (Private Sector) Act 2000* and the APP's) apply to ALL health service providers in the private sector, regardless of whether or not any separate State or Territory legislation exists and regardless of the annual turnover of the business. Therefore all ATMS accredited Practitioners must make sure they comply with the applicable requirements of the Privacy Act and the APP's as well as any Commonwealth, state or territory legislation that may also apply.

- ***What is personal information? Do I collect it?***

Personal information is information or an opinion about an individual that could allow someone to reasonably identify the individual from the information or opinion. The information or opinion does not have to be true.

- ***What is sensitive information? Do I collect it?***

"Sensitive information" includes information or an opinion about an individual's racial or ethnic origin, religious beliefs or affiliations, philosophical beliefs, health information, biometric information and/or sexual orientation or practices. In the course of work undertaken by ATMS members and health practitioners, it is noted that sensitive information may be collected, used and stored. The Privacy Act and APP's place additional obligations on business' that collect sensitive information.

- ***I am a sole operator self employed natural medicine practitioner and my business does not have an annual turnover of $3 million. Does the Privacy Act and the APP's apply to me?***

Yes. All organisations that provide a health service are covered by the Privacy Act whether or not they are small businesses and regardless of the organisation's annual turnover). Additional State or Territory legislation might also apply. If in doubt you should obtain independent legal or expert advice.

Organisations providing a health service include natural medicine practitioners such as naturopaths, massage therapists etc. **All Practitioners accredited by ATMS are subject to the Privacy Act and APP's.**

- ***How do I deal with privacy if my practice is integrated or multi-modality?***

If your practice or clinic is integrated or multi-modality, implied consent may be sufficient to share information between practitioners within the practice. However, a safer option is to

obtain the patient's or clients' express consent during the initial consultation to share this information. It is also recommended that where possible this is dealt with in a privacy policy.

- ***I work in a health food shop or pharmacy. My job is to talk to people in the general public area. I don't do full consultations and therefore do not consider I am working as a natural medicine practitioner. Do I have any Privacy obligations?***

In most cases, the answer is yes. When you collect a person's personal or "sensitive information" or discuss their symptoms with them, the person may have concerns about discussing their health issues in public and how the information provided is recorded, handled and stored. Where conversations may be overheard, they should be conducted in a manner sensitive to the surroundings. Depending on the circumstances, you may need to take additional steps to protect the person's privacy, such as taking them to a more private area. Be mindful that even calling out a person's name might be inappropriate in some circumstances.

- ***How long do I need to keep a patient's records for?***

Perhaps the most common question and there are unfortunately various answers.

Most of the State and Territory Privacy Legislation require that records be kept for a minimum of 7 years from the date in which the Practitioner last provided services to the patient/client. In the case of treatment provided to a child, (anyone under the age of 18), the records must be kept until the person has reached the age of 25. Medical providers and Practitioners are advised to consult the relevant State and Territory legislation or registration and obtain legal advice if they are unsure.

For example, the Chinese Medicine Registration Board however requires that Chinese Medicine practitioners in Victoria maintain records for at least 12 years', and longer if possible.

The ATMS position is that records be securely maintained for at least 12 years', or until the person turns 25, whichever is the longer period. If however you can reasonably and securely store the records for a longer period, then this should be considered.

However should a patient request you destroy his or her records, you must check the specific legislation that applies in your situation and if destruction is permitted under that specific legislation, you must act to securely destroy the records.

- ***Who 'owns' the records, me or the clinic owner?***

Perhaps the second most common question and the one that causes most angst.

Unfortunately there is no clear answer which will apply in all cases, and who has the responsibility for a patient's records will depend on the facts of each individual circumstance. In some instances it might be that the person who wrote the records that holds responsibility

for the records. In some other instances the clinic owner might more properly be responsible for the safe storage and ongoing access to the records.

However an overriding consideration is always that the person to whom the records relate must be able to have access to the records. So in reality the question is not who owns the records, but who has the responsibility for securely storing the records for the required period and for subsequently ensuring the patient/client can have access to those records if requested.

Disputes about who is to maintain a person's records are best prevented, rather than attempted to be 'cured'. In this regard, other Privacy considerations are useful. As explained in the next two questions, what a person should be told at time of collection and what information should be contained in the mandatory Privacy Policy should also prompt and guide practitioners and clinic owners in ensuring that this question of who is responsible for a person's records when a practitioner leaves the clinic is addressed at the time the person's health information is first collected.

In particular the APP's make it clear that "Advising the individual, at the time health information is collected, about how the health service provider will handle their information is an important part of protecting privacy." This guidance from the Office of the Australian Information Commissioner would apply to ensure that the person is made aware of what will happen to their health records if the practitioner should leave the clinic.

Accordingly prevention may always be achieved by the clinic owner and the practitioner establishing clearly and in writing before any problems arise as to what will happen with a patient's records once the relationship between the practitioner and clinic owner ends. This agreement should then be reflected in the clinic's Privacy Policy and also reiterated in the information provided to each person at the initial consultation regarding the collection, access etc of their private health information.

What if there is no agreement and a dispute arises?

Again it must be stressed there is no black and white answer, and each case will depend on its individual merits. However always remember that the overriding consideration is that the person to whom the records relate must be able to have access to the records. Consequently if at all reasonable one suggestion is that the parties agree to seek the patient's wishes as to who should now store the records, and those wishes should be recorded and followed if there is a dispute. This however is only a suggestion, and may not be suitable or appropriate for all cases.

And a final word here. Remember that under the APP's, a person's health records may only be used for the purpose they were obtained. This will generally exclude most marketing initiatives unless consent is obtained for this purpose.

What should I tell a patient about my collection of their health and other information?

At the time he/she collects the information, or as soon as practicable afterwards, a health service provider should take reasonable steps to make the individual aware of a number of things including:

- ✓ the identity of the organisation and how to contact it;
- ✓ the purposes for which the information was collected;
- ✓ what organisations the information could be given to;
- ✓ the fact that the individual can access the information held by the provider;
- ✓ any law that requires the particular information to be collected; and
- ✓ the main consequences (if any) for the individual if all or part of the information is not provided.

This information should be outlined in a detailed privacy policy which is provided to clients and patients, whether they are current, former or potential. If you have a website you should also provide a link to your current privacy policy on the website.

What is 'practicable' and what is 'reasonable' will depend on the circumstances. For example, these may relate to the costs involved, or the circumstances of collection such as whether the information is collected in an emergency.

Do I need to have a Privacy Policy?

Yes. Under the Privacy Act and APPs you are required to develop a document explaining how you handle personal information. This document is often referred to as a Privacy Policy. The APP's stipulate what must be included in a Privacy Policy and how the policy can be accessed.

Most ATMS practitioners are self employed sole or small operator healthcare providers. Consequently most ATMS practitioners would be able to rely on a privacy policy explaining, in simple terms, how and what information is collected and the privacy safeguards the practitioner/practice has in place to protect information, and other information required to be included under the APP's. The APP's also require businesses to implement a Compliance Plan, which outlines how the business will comply with their obligations under the Privacy Act and the APPs.

The Privacy Policy can be made available in a number of ways, depending on what is most effective in the circumstances. For example, it is common to upload the privacy policy onto the website, or it could be on a sign in the practice or in a printout or a pamphlet that could be handed out by the health service provider if someone asks for it.

When deciding how best to make the policy available, a key factor will be to ensure that individuals are able to readily access and as far as possible be able to understand the policy. For example, additional assistance or explanation may be needed for people whose first language is a language other than English, people with disabilities or for people with literacy difficulties. As not all individuals have access to a computer or the Internet, a policy placed

only on a website may not be sufficient and you will need to make the policy available in other forms if reasonably requested by an individual.

What is the purpose of a privacy policy?

It is important that entities respect their client and customers privacy. The Privacy Act stipulates that all APP entities must have a privacy policy. A privacy policy should detail how an entity collects, uses, discloses and stores an individual's personal information to ensure privacy is maintained.

What is required to keep records securely?

Some reasonable physical safeguards might include:

- ✓ Locking filing cabinets and unattended storage areas
- ✓ Physically securing the areas in which the health information is stored
- ✓ Not storing personal information, sensitive information or health information in public areas
- ✓ Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public.

Some reasonable technical safeguards might include:

- ✓ Using passwords to restrict computer access, and requiring regular changes to passwords
- ✓ At least one back up of personal information, sensitive information and health information is stored on a physically separate drive, and this back up drive is kept securely and with all the protections applying to the source drive
- ✓ Establishing different access levels so that not all staff can view all information
- ✓ Ensuring information is transferred securely (for example, not transmitting personal information, sensitive information or health information via non-secure email)
- ✓ Using electronic audit trails
- ✓ Installing virus protections and firewalls.

Some reasonable administrative safeguards might include:

- ✓ Introducing appropriate policies and procedures to address information security
- ✓ Training staff on those policies and procedures
- ✓ Introducing a Privacy Compliance Plan.

What does access to records mean?

Access may be provided in a number of different ways. This may include but is not limited to:

- ✓ Giving the person a copy of the personal information
- ✓ Providing a reasonable opportunity for the patient to inspect the personal information, take notes on its contents and talk through the contents with an appropriate staff member, if required

- ✓ Allowing the person to listen to or view the contents of an audio or visual recording
- ✓ Giving the person a print-out of the personal information if it is stored electronically, or giving them an electronic copy of the information.

Exceptions to this might occur if it would result in an unreasonable financial strain, be detrimental to the preservation of the information or involve an infringement of copyright. If so, access should still be provided in some other convenient form.

Can access be refused?

- ✓ Access may be refused in some limited circumstances.

The Privacy Act requires, and ATMS expects, that the person seeking access will be given written reasons as to why access has been denied. ATMS further expects that an ATMS practitioner would advise the person that if they felt the decision by the practitioner was unreasonable they may contact ATMS or the Office of the Australian Information Commissioner to inquire about lodging a complaint.

What if a record needs to be amended?

The first guiding principle here is that if a record is found to contain information that is incorrect, misleading, irrelevant, out of date etc, then it must be corrected. If there is disagreement about the accuracy of the information, the practitioner should request a statement setting out the patient's concerns with the information in question.

The second guiding principle is that the correction should if possible be carried out in such a way that it is possible to identify what it was that was corrected. This means that the use of correcting fluid, tape, erasures etc should be avoided. The incorrect record should be annotated in such a way that it is still legible but which clearly shows that it is subject to a correction. The correction must then be entered and clearly identified as correcting the relevant section. If a large section needs correcting, for example an entire page, it will generally be most useful to write an entire new record, but keeping the old record attached to the new.

Can I charge for access and/or correction to a record?

ATMS encourages practitioners to provide access and amendment to a patient's records without charge. However you may charge an administrative fee to a patient to cover the cost of providing them with details of the personal information you hold about them. The fee must not be excessive and must not discourage a person from seeking access to their records. ATMS expects that if charged, any administrative fee would be unambiguously reasonable and able to be fully justified.

Practitioners **cannot** charge a patient a fee for correcting their records.

- ***Can I share a patient's health information with another person or practitioner?***

The various pieces of Legislation provide quite a wide range of rules and conditions which must be applied when sharing health information. The general rule to apply is to always fully explain to the patient why you wish to share their information, and what information will be shared, and then obtain the patient's written permission before you divulge any of their health information to any person.

If you work within a multi-disciplinary/practitioner team it is often necessary to share information to deliver optimum health care. When first collecting information, the patient should be advised of this fact, and you should discuss with the patient how this approach to treatment will affect the handling of their health information. That this disclosure occurred, and the outcome, should be recorded in writing and acknowledged in writing by the patient.

In the very rare (for a natural medicine practitioner) circumstance of an emergency, health information may be disclosed without prior permission. There are limitations however that still apply and you should seek independent legal advice or contact the Office of the Australian Information Commission if in doubt.

- ***My records for a patient contain information which was given to me by another practitioner 'in confidence'. Do I need to provide access to this information?***

Yes. Access to information may only be refused if specifically allowed for under the relevant legislation. See "Can access be refused?" above.