Australian Traditional-Medicine Society Ltd

THE PRIVACY ACT AND THE AUSTRALIAN PRIVACY PRINCIPLES

PRIVACY GUIDELINES FOR ATMS MEMBERS

1. INTRODUCTION

Healthcare practitioners (**Practitioners**) from all modalities – allopathic and natural – are bound by the *Privacy Act 1988* (Cth) (**the Privacy Act**). This includes incorporated entities and individuals (e.g. ABN holders). Practitioners are also bound by other relevant state and territory privacy laws, however the ATMS Guide below will focus on the Privacy Act only.

2. THE *PRIVACY ACT 1988* (CTH) AND THE APP'S

- From 12 March 2014, changes to the Privacy Act meant that **13 Australian Privacy Principles** (**APP's**) were introduced which replaced the previous National Privacy Principles and Information Privacy Principles.

- The APP's apply to government agencies and to private sector organisations that have an annual turnover of $3 million or more.

- Regardless of their annual turnover, private sector health service providers are also covered and must also comply with the APP's and the Privacy Act. This includes Practitioners.

Australian Traditional-Medicine Society Ltd (**ATMS**) provides the following guide to ATMS member Practitioners. The guide is intended to provide an overview of the APP's and outline some general information on how the APP's apply and operate, and what is required of Practitioners when dealing with an individual's personal information. It is not legal/expert advice and it is intended to be used as a reference and guide only, by Practitioners when developing their own policies. Practitioners should obtain independent legal/expert advice if they are in doubt as to their precise obligations. ATMS may be able to assist to refer to you the appropriate person, please contact Karen Seaton for further information.

This guide will focus on Practitioner's obligations under the Privacy Act at a Federal level and will not comment on the Practitioner's obligations under the relevant state and territory legislation.

3. THE PURPOSE AND CONTENT OF A PRIVACY POLICY

- Due to the nature of the work performed and services provided by ATMS members, Practitioners will collect, access, use and handle personal information from clients, including former and potential clients, and other individuals that they deal with on a regular basis.

- All APP entities (this includes Practitioners and ATMS members) must have a privacy policy that details how they manage personal information.

- Personal information means information or an opinion about an individual, whose identity can be directly or indirectly apparent or reasonably ascertained from that information or opinion, whether that information or opinion is true or not.

- Privacy Policies must be clearly expressed and up to date.

  The APP's state that a privacy policy must contain and detail:

  a) The kinds of personal information the Practitioner collects and holds;
  b) How the Practitioner collects and holds personal information;

c) The purpose for which the Practitioner collects, holds, uses and discloses personal information;
d) How an individual may access the personal information held by the Practitioner and seek the correction of such information;
e) How an individual may complain about a breach of the APPs and how the entity will deal with such a complaint;
f) Whether the Practitioner is likely to disclose personal information to overseas recipients;
g) And if the Practitioner is likely to disclose personal information to overseas recipients, the countries in which those recipients are likely to be located if it is practicable to specify those countries in the policy (often it is difficult to fully specify as third party IT providers may have services in more than one country which you are not aware of).

- It is recommended that Practitioner's seek legal advice if they are unsure on the information that is required to be included in a Privacy Policy and the associated Privacy Compliance Plan (which is also required).

- Practitioners should note that some of the above information is "sensitive information" for the purposes of the Privacy Act, and care should be taken in the collection, use, handling and storage of such information.

- Sensitive Information includes information or an opinion about an individual's:

  - Racial or ethnic origin;
  - Religious beliefs;
  - Philosophical beliefs;
  - Sexual orientation or practices;
  - Health information about an individual.

- The APP's stipulate that entities that collect, handle and use "sensitive information" must take extra measures when collecting, using and storing such information. Practitioners should be aware of these extra obligations, as many will collect, handle and use sensitive information.

- When collecting personal information (which includes sensitive information), it is recommended that Practitioners explain to the individual how this information influences diagnoses and treatment. It is a requirement of the APPs that Practitioners detail all types of personal and sensitive information collected.

- Practitioners must take reasonable steps to ensure practices, procedures and systems are implemented within the entity (whether corporation or an ABN business holder/individual) to ensure compliance with the APP's and outline how the entity/individual will deal with any complaints or enquiries in relation to the privacy policy.

- This is commonly dealt with by an internal Compliance Plan, and all ATMS members and Practitioners should ensure something of the like is implemented and monitored.

4. DEALING WITH CLIENT'S PERSONAL AND SENSITIVE INFORMATION

- Individuals have a right to refuse to share personal information to Practitioners. Practitioners should explain to any individual that a refusal to share personal information can mean that the Practitioner is unable to provide the client with the appropriate treatment.

- Clients and individuals have the right to deal with Practitioners anonymously, or by using a pseudonym, provided this is lawful and practical. Practitioners should however understand that in the healthcare context, this is unlikely to be practical or possible for the purpose of insurance rebates.

- Practitioners are likely to collect, use, access and store government identifies including but not limited to Medicare numbers and details. Practitioners must make it clear in their privacy policies that such identifiers will be appropriately dealt with and handled, and used only to fulfil obligations to the relevant government agencies and ensure such practices are implemented in practice.

5. THE USE OF PERSONAL INFORMATION FOR THE PURPOSES OF MARKETING AND ONLINE

- Practitioners may collect personal information for marketing purposes. The collection of this personal information may enable Practitioners to contact individuals (being clients or otherwise) via mail, telephone, e-mail, sms message or through social media channels to update individuals about services, products and specials. We note many clinics and Practitioner's may have a regular newsletter and e-mail mail-outs (for completeness, we note that the sending of e-mails is regulated by the SPAM Act – not the Privacy Act, however, similar provisions regarding the use of personal information and the need to obtain consent to send marketing material apply under the SPAM Act and the Privacy Act).

- Practitioners must give individuals the option to consent or refuse to the use of their personal information for direct marketing purposes, and to withdraw their consent at any time. Practitioners must ensure that individuals are provided with contact details on how to unsubscribe.

- Practitioners must also be aware that even if an individual 'opts out' of receiving marketing materials, individuals may still be contacted for the purpose of sending accounts, appointment reminders etc.

- Practitioners should also note their obligations under the Spam Act 2003 (Cth).

- When individuals visit a Practitioner's website, certain information such as the time, date, browser type, operating system, website visited immediately before coming to our site, etc may be collected. Such information is usually collected through "cookies".

- Practitioners should make it clear that such information is used only in an aggregated manner to analyse how people use our site so that we can improve our customer service and to make the website easier and more efficient to use.

- If the website has links to other sites, Practitioners should consider including a disclaimer to the effect that they are not responsible for external sites or the consequences of accessing those sites from the Practitioner's website.

6. STORAGE & DISCLOSURE OF PERSONAL INFORMATION

- Practitioners should take note on how personal information is stored in their clinics and business. For example, Practitioner's may store personal information in hard copy, on a computer, on a mobile device such as a smart-phone or tablet or on a combination of the above.

- Practitioners should take all reasonable steps to ensure that personal information is stored securely and is protected from misuse and loss; and from unauthorised access, modification or disclosure. Measures to ensure the security of personal information includes a range of systems and communication security measures, as well as the secure storage of hard-copy documents.

- Practitioners should also take steps to ensure that access to personal information is restricted only to those who are properly authorised to gain access. Clients and individuals should be made aware to this.

- The Office of the Australian Information Commissioner Fact Sheet has practical suggestions on how to keep personal information and data secure. Practitioners must be able to detail the security measures taken. This should be set out in a Privacy Compliance Plan. A Compliance Plan must also address how the Practitioner will deal with complaints and enquiries from individuals.

- It is recommended that Practitioners retain their clients' health records for a minimum of 12 years after their initial visit. After that time, if the record is no longer necessary, practitioners should make it clear in their privacy policy that the personal information will be disposed of securely as required by law. It is recommended that the health records of children (defined as under age 18) should be kept until they turn 25.

- Except for certain situations, Practitioners should never give or disclose personal information to third parties without obtaining the individual's express consent. This includes sharing the personal information with other health practitioners who may be involved in the individual's care. This should be done only if the practitioner obtains the individual's written permission to do so.

- In some situations, it may be necessary to share personal information outside an organisation. Such situations include but are not limited to:

  - Where practitioners are required by law to disclose the information (e.g., reporting of communicable diseases).
  - To provide necessary follow-up treatment and ongoing care.
  - To address liability indemnity arrangements with insurers, medical defence organisations and lawyers.
  - For the defence of anticipated or existing legal proceedings.
  - To process private health fund claims.

  Practitioners should obtain consent up front when they first see/treat an individual highlighting that such circumstances may arise (however unlikely) and that individuals agree to disclosure in such circumstances.

- If an individual believes that their personal information (including sensitive information) held by a Practitioner, is inaccurate, out of date or incomplete, they have the right to request to review the information.

- The APP's outline when and how a Practitioner must respond to an individual's request to access and view personal information (which includes sensitive and health information) held.

7. OVERSEAS DISCLOSURE OF PERSONAL INFORMATION

- The APP's have stringent requirements for entities that disclose personal information overseas.

- Practitioners should think very carefully about the disclosure of personal information to overseas recipients. The first reaction is that this doesn't apply, and that no personal information is collected, used or handled by off-shore recipients. However, with the growth of international freelancing sites, Practitioner's may decide to outsource accounting functions, change to Cloud Computing, use overseas secretarial services, have transcriptions done overseas, have a website designed or managed by an overseas company, and/or use an internet server that is located overseas.

- There are numerous and increasing possibilities with technology advancements, so Practitioner's must ensure that they are definitively aware of any personal information that is disclosed overseas and ensure compliance with the APPs.

- If personal information is disclosed to overseas recipients, Practitioners must take reasonable steps to ensure that the overseas recipient entity does not breach the APP's in relation to the personal information disclosed. Privacy policies may also have to include a list of the countries in which the personal information is disclosed to. A breach of the APP's by the overseas entity may be considered a breach by the Practitioner.

8. MODIFICATIONS TO A PRIVACY POLICY

- Privacy policies may be modified at any time and it is recommended that Practitioners regularly review the policy to account for any legislative or societal changes or changes in the running of the Practitioner's business and operations and seek the appropriate legal advice when required.

- When amending policies Practitioners are advised to keep clients and other individuals updated on such changes. This could be include the updated, amended version being posted on the Practitioners website or having the policy available in the Practitioner's clinic or firm.

9. WHAT YOU NEED TO DO

- It is recommended that Practitioners review their privacy policies and the internal procedures on how personal and sensitive information is collected, handled, used and stored. Penalties apply for breaches of the APP's and the Privacy Act.

- If you have any questions or concerns about this guide, or privacy issues in general, please contact ATMS for further information.