ESOTERIC PRACTITIONERS ASSOCIATION

EPA Privacy Policy Guidelines

February 2018

ESOTERIC PRACTITIONERS ASSOCIATION PTY LTD | ABN 75 139 603 160
15 Blue Hills Avenue, Goonellabah NSW 2480 Australia | office.au@epa-international.com | P 02 6624 3706 | F 02 6624 3702

WHY THE NEED FOR A PRIVACY POLICY?

In short, you are required as a health-care provider to handle your clients' personal and sensitive information in accordance with law. This is part of your duty of care to your client. Hence knowing what the law is in relation to this, is important. The purpose of these guidelines is to support in this regard, however, as with all aspects of your practice, your responsibility to stay up to date with the laws and regulations applicable to your area of practice, is your own.

Significant amendments to the Privacy Act 1988 (Cth) that regulates the handling of personal information became operative on 12 March 2014 and include the requirement for defined businesses to follow the 13 Australian Privacy Principles (APPs). Those defined businesses include businesses providing a health-care service. All EPA members are expected to comply with current law affecting their practice and hence would no doubt already be aware of the APPs.

It is important for members to be aware of current requirements and to update their privacy policies accordingly. As of 1st February 2018, this includes updating Privacy Policies to include new Data Protection Laws.

This document aims to bring an understanding of how to ensure that you as a practitioner adhere to the privacy laws, which include data protection.

Who must abide by the Privacy Act?

The Privacy Act must be observed by those people who are:

- Working in Australian Government agencies (e.g., Commonwealth Rehabilitation Service, Centrelink)
- Contracted to provide a service to the Commonwealth Government
- Working in businesses with a turnover of more than $3 million
- Working in private health services, defined as those which:
    - o Assess, record, maintain or improve an individual's health, or
    - o Diagnose the individual's illness or disability, or
    - o Treat the individual's illness or disability or suspected illness or disability.

The regulation of privacy also applies to all small business operators who provide a health service and hold health information. Examples of health information include:

- Notes of an individual's symptoms and the treatment given
- Specialist reports and test results
- Appointment and billing details
- An individual's health-care identifier when it is collected to provide a health service
- Any other personal information (such as information about an individual's race, sexuality, religion, date of birth, gender), collected to provide a health service.

For a sole operator or small business, the above documentation can be kept very simple and include a brief description of your procedures for handling the personal information in your care. We have completed a Privacy Policy Template for you to adapt for your business.

EPA PRACTITIONER RESPONSIBILITY

As with all EPA matters, it is a condition of your recognition that you comply with all relevant laws and regulations. Equally, the EPA Code of Ethics and Conduct asks practitioners to take the privacy of clients seriously as it is a vitally important part of their duty of care and confidence to comply with all relevant legislation and it is your responsibility to ensure you are aware of the requirements of the 13 APPs, and updates to legislation as they occur from time to time, and develop the requisite policy and procedures for your practice and clinic.

While it is the personal responsibility of each practitioner to inform his or her self and to comply with all relevant legislation, the purpose of this document is to inform and bring to your attention your requirements to follow these 13 APPs.

What is required of you?

There are three separate obligations on an operator or business:

- To implement procedures that will ensure you comply with the 13 APPs and are able to deal with related inquiries and complaints
- To have a clearly expressed Privacy Policy about how you manage personal information (it is your responsibility to develop this), and
- To take reasonable steps to make your Privacy Policy available free of charge where requested.

We have also completed for you the guidelines for the new data protection Laws EPA Data Protection Guidelines along with the already mentioned EPA Privacy Policy Template.

WHAT ARE THE 13 APP'S RELEVANT TO THE PRIVACY ACT?

The Office of the Australian Information Commissioner (OAIC) has written a set of APP guidelines that you must be aware of. They can be found on: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

The 13 Australian Privacy Principles (APPs) are concerned with the collection, storage, use, access, disclosure and destruction of personal information, as well as how a person/client can access and change their information or make a complaint. These are basic rights which clients have – and are both basic and easy to comprehend and respect given that the information is theirs (the client's), and relates to their health. Therefore, as an EPA member operating to the standard of the EPA Code of Ethics and Conduct, the need to protect such information will be obvious to you. All such information is required to be retained in secure storage such that it is only accessible by properly authorized persons.

Below is a summary of the key principles of the Privacy Act. You are expected to be familiar with them and apply them to your practice.

APP 1: Open and transparent management of personal information

There is expanded prescribed information that health practitioners must include in their privacy policies for clients. Privacy policies must refer to:

- The kinds of personal information collected
- How that information is collected and held
- The purposes for which that information is held, used and disclosed
- How a client may access and seek correction of their personal information
- How a client may complain about a breach of the APPs
- How you will deal with such a complaint
- Whether you are likely to disclose personal information to overseas recipients, and if so, the likely countries.

Health professionals must take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs, including training staff if applicable and establishing procedures to identify and manage privacy risks.

Link to APP 1 ~ https://bit.ly/2RiiGxJ

Action Required:

Review and update your privacy policy, practices and procedures to ensure compliance with the APPs guidelines, including introducing systems for handling clients' privacy inquiries and complaints. Make your privacy policy available to clients in an appropriate form, whether on line and or have copies available should a client ask to read your privacy policy.

APP 2: Anonymity and pseudonymity

Health professionals must give individuals the option to interact with them anonymously or by using a pseudonym, unless it is impracticable, or where the law or a court order requires clients to identify themselves.

Examples of where the right to anonymity or pseudonymity could arise in a health-care context include where a person makes a phone call to your clinic to enquire about the services provided, or where someone purchases a product from you in a retail environment over the counter. In such cases, they have the right to do so anonymously or pseudonymously; in other words, they do not need to give you their name and contact details.

A further example is that if a person signs up to an email list of a practitioner, they are not required to give their real name. They will, of course, be required to give a valid email address in order to receive the email service, but they have a right to give a pseudonym (if your site asks for a name).

In certain cases, it will be impracticable to provide the relevant service if the person does not provide personal information. For instance, if you are shipping purchased product to the client, you will need a name and address to ship to.

In relation to provision of a health-care service, circumstances where an individual may choose to remain anonymous could for instance include:

- When they live in a small country town
- For insurance purposes, as sometimes seeing a health professional could impact the person's insurance

- In relation to incidents of domestic violence
- In relation to incidents of sexual abuse (however note that mandatory reporting requirements can apply).

In the case of EPA practitioners, you should also note that it is not a requirement that practitioners seek proof of identity and hence it will not always be possible for you to be aware if you have been given a pseudonym or whether your client wants to remain anonymous unless they inform you of this fact. Therefore, the exception to anonymity and pseudonymity (for impracticability) would hold more relevance to practitioners operating a service where proof of identify is required, such as those instances where Medicare rebates, WorkCover or other insurance considerations apply. Nonetheless, it still should be considered, so as to ensure you are meeting your obligations.

In relation to the provision of a health-care service, it may be unusual for a client to request anonymity or pseudonymity, however you should be aware that this is permitted by law. In the case of a registered medical service, as referred to above, disclosure of personal information is required in order to receive Medicare or private health insurance rebates, however this is not applicable to an EPA recognised practitioner, as no rebates are applicable. Notwithstanding this, the use of anonymity or pseudonymity is permitted as long as this is lawful and practicable.

Therefore, be very careful before denying a client the right to anonymity or pseudonymity, as the law is very strong on clients' rights in this regard.

As well as considering the client's rights, part of the practicability and lawful considerations for you as practitioner are that proper records must be kept by a health-care professional under law, and for continuity of health-care to be provided. However, a court is likely to give weight to the client's right to anonymity and pseudonymity (although there would no doubt be exceptions).

Ultimately, it is up to you as a health-care professional to ensure you meet all relevant requirements. This remains your responsibility and is not something the EPA will or can take on for you. However, we are there to discuss this with you and provide our support should such a situation arise. Hence, if you receive such a request from a client and are unsure, please contact the EPA for any updates or suggested contacts.

Can you refuse to provide a health-care service?

The simple answer is, yes you can, but you should be acting reasonably and not discriminating in doing so.

For instance, a doctor can refuse to see a patient, as long as the person's life is not in danger and requires urgent medical treatment. If a client (or potential client) requested treatment from you and wished to remain anonymous, you would need to assess the situation at hand. In such circumstances, it would be likely that you, as an EPA recognised practitioner and not a registered medical practitioner, would not be the appropriate person to treat the person and therefore you would be required to refer them to emergency, registered medical care. The same principles apply in relation to all clients presenting conditions – if they are outside your scope of expertise, or if you are not the appropriate practitioner in the client's best interests, then you must put your client's interests first and refer. Read the EPA Code of Ethics and Conduct in relation to referral.

In non-emergency situations, if you honestly and reasonably believe that you are not the appropriate practitioner to see a client, you may refuse to treat them, for instance if you feel you cannot help them, if they are an existing client and you feel the relationship has broken down, or seeing (or continuing to see) a client would breach professional boundaries. These are all important considerations. However, if you refuse to see a client, you must not breach discriminatory laws in doing so. See the Australian Government business website for further information on discrimination laws: https://bit.ly/2BGIYjg

A useful reference in relation to refusing to see a patient is located on the NSW Health Care Complaints Commission website, https://www.hccc.nsw.gov.au/health-consumers/frequently-asked-questions-health-consumers/does-a-practitioner-have-to-see-a-patient

Note that this applies to doctors, and therefore is not directly applicable to EPA recognised practitioners, but the principles are clearly laid out and should be read.

APP 2 link ~ https://www.oaic.gov.au/assets/privacy/app-guidelines/APP-Guidelines-Chapter-2-v1.1.pdf

Action Required:

Provide practices, procedures and systems to enable your clients to interact with you anonymously or by using a pseudonym, where this is desired by the client, and is practical and legally appropriate. If you do not feel comfortable providing an anonymous service for whatever reason, you have the right to decline service, as long as you are not being discriminatory. See above for relevant points.

APP 3: Collection of solicited personal information

This APP stipulates that the collection of sensitive information should not occur except in "permitted health situations", or if an individual consents to the collection. Health information is included within the definition of sensitive information, and one of the permitted health situations is "the collection of health information to provide a health service".

APP 3 link ~ https://www.oaic.gov.au/assets/privacy/app-guidelines/APP-Guidelines-Chapter-3-v1.1.pdf

Action Required:

As a health professional you may need to collect sensitive information however you must ensure that you follow the requirements as set out in APP 3.

Sensitive Information is a subset of personal information and includes your health information as well as information pertaining to racial or ethnic origin, political opinions or membership of a political organisation, religious belief or affiliations, membership of a professional or trade association, sexual preferences or a criminal record. Sensitive information attracts additional privacy protections compared with other types of personal information.

As health care providers, you gather sensitive information which includes information about the health or a disability (at any time) of an individual, or an individual's expressed wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual, or other personal information collected to provide, or in providing, a health service.

It may also include information about an individual's physical or mental health, notes of an individual's symptoms or diagnosis and the treatment given, specialist reports and test results (in the case that a client has given you a copy – these should never be requested), appointment and billing details and/or medication details. This relates to APPs 3 and 6.

APP 4: Dealing with unsolicited personal information

This APP describes those occasions in which you receive information that you have not asked for.

If you could not have gathered that information under APP 3 and it is not in a Commonwealth record, then "it must be destroyed or de-identified if it is lawful and reasonable to do so." In circumstances where the information could have been collected under APP 3, or it is in a Commonwealth record, then does it not have to be destroyed and must be managed as described in the APPs 5 to 13. Unsolicited information includes misdirected mail that you have received, an employment

application from an individual under his or her own initiative (not in response to an advertisement you have placed for a job vacancy) or promotional material sent to you.

APP 4 Link ~ https://www.oaic.gov.au/assets/privacy/app-guidelines/APP-Guidelines-Chapter-4-v1.1.pdf

Action Required:

APP 4 is a situation that is not likely to arise, but it requires discretion and care. If this information is retained, it must be because it relates to the purpose of your service to the client and it may only be used for the purpose for which it was given to you, it must be treated securely, and the individual to whom it relates may request access to it and its correction. The main point is that if a practitioner receives information that they have not asked for and it does not relate to the service being provided then they should destroy/de-identify it. Exceptions would include if there is a mandatory reporting requirement.

APP 5: Notification of the collection of personal information

Health professionals must notify their clients about the access, correction and complaints processes in their APP privacy policies.

APP 5 link ~ https://bit.ly/2LDMqQ8

Action Required:

Review your informed consent policies to be sure that clients are clear about the personal information you will be collecting. Refer to the EPA Code of Ethics and Conduct section 4.3 for Informed Consent guidelines. Part of your obligations in seeking informed consent is in ensuring that your clients are informed about the services you provide and what they can expect. In addition under this APP, your clients need to know that they have the right to request access to their information and to correct it, as well as how to make a complaint if they want to about how their personal information has been handled, and how this will be treated if so. You could develop a policy for this purpose outlining the client's rights to access and your procedures in that regard.

APP 6: Use or disclosure of personal information

This APP states that personal information can only be used for the purpose for which it was collected. For example, a health care practitioner will gather the personal information about a client's health status that helps them to provide the correct treatment for that client (Primary purpose). Secondary use or disclosure is only allowed in very specific circumstances, all of which are detailed in the link given below. Health professionals may disclose personal information if a "permitted general situation" exists such as to "lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety". The key change from the previous National Privacy Principles (NPPs), which were replaced by the APPs, is that the threat no longer needs to be imminent. Another allowable disclosure is when it is necessary to assist in locating a missing person.

APP 6 link ~ https://bit.ly/2CF8Gq5

Action Required:

Use the personal information you gather for its primary purpose. If you intend to use this information for a secondary purpose you must seek legal advice. You may be required to de-identify the information before disclosure. Be clear with your clients that there may be occasions when you may disclose their personal information where there is a serious threat to the life, health or safety of an individual or the public, or on a rare occasion to assist in the location of a missing person.

APP 7: Direct marketing

This APP applies to any material you send to your clients to promote your services, or goods you sell. This is material sent to a person, by name and to their address. It does not include un-named and unaddressed flyers delivered to letterboxes.

APP 7 link ~ https://bit.ly/2VgZkbs

Action Required:

This APP states that you should not use the personal information you hold about a client in any direct marketing, unless they reasonably expect it to be used. It is recommended that you refrain from using detailed personal information for these purposes.

You should ensure that your clients have the choice to 'opt-in' to marketing. This means that you do not automatically send them marketing; best practice is to ask them (e.g. when they first see you or inquire on your website etc) whether they would like to receive marketing material (including any e-newsletter or the like) from you. This can be done as simply as through a check-box which they select to indicate their 'signing up' or opting in to any such notifications or marketing. You must also provide a simple means for clients to 'opt out' of direct marketing once they have signed up. Therefore, you should give them the opportunity to unsubscribe from such marketing, or change their preferences, at any time. Your website may contain such functionality or you may simply let them know they can email you (at a specified email address) if they want to unsubscribe or change their preferences.

APP 8: Cross-border disclosure of personal information

This APP applies to information that is sent to an overseas recipient. You are responsible for ensuring that the recipient handles the personal data in accordance with these APPs, primarily APP 6, which states that information is used for the primary purpose for which it was collected.

APP 8 link ~ https://bit.ly/2M1otF7

Action Required:

This APP applies if a client is moving overseas and their treatment records are transferred to a practitioner in that nation. It is recommended that you take 'reasonable steps' to ensure that personal information is handled in accordance with these APPs.

It would be prudent to ask for the Privacy Policy of that practitioner before records are sent to them. This should include the ways they collect, use, disclose, destroy or de-identify data, their processes for handling privacy complaints and their data breach response plan.

APP 8 also applies to the use of testimonials on your website/s, where that information is accessible to international recipients. It is recommended that no personal information about clients is disclosed on your website/s, and that the people who make testimonials for your website are de-identified and, in any event, no testimonials are shared publicly, on any forum, without the client's prior written consent. Note, certain medical professionals are not able to use testimonials in any way shape or form due to the regulations of their governing bodies. This applies for example to registered medical practitioners, under AHPRA, if you are unsure consult with your EPA Committee or your insurance body.

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

A government related identifier is a 'number, letter or symbol, or a combination of those things that is used to identify an individual or to verify the identity of the individual' and 'that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract', for example, a client's Medicare number.

APP 9 link ~ https://www.oaic.gov.au/assets/privacy/app-guidelines/APP-Guidelines-Chapter-9-v1.1.pdf

Action Required:

These identifiers are not to be collected by EPA members under any circumstances.

EPA members are not recognised to provide any service that would require use of a government related identifier. By way of example, EPA recognised therapies are not eligible for Medicare, nor to offer private health insurance rebates. Hence there is no reason why an EPA recognised practitioner would require such information. The principle of privacy of a client's data starts with the premise that, if you do not need it in order to provide the health-care service, then you do not collect it.

The exception, of course, is if an EPA member is also a practitioner of a service to which such a government identifier relates. However, in that case, the identifier would be collected by virtue of that other (e.g. registered) health-care service. The important point with such practitioners is that the two services must never be mixed, and under no circumstances whatsoever should an EPA member ever afford a benefit ascribed to a registered medical (or other relevant) service, to an EPA recognised therapy, where that therapy would not be eligible for such a benefit. Do not mix the two.

APP 10: Quality of personal information

Health professionals must take reasonable steps to ensure that the personal information that they collect, use or disclose is up to date, accurate and complete. The personal information used or disclosed must also be relevant to the purpose of the use or disclosure.

APP 10 link ~ https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/

Action Required:

Review your record keeping practices, procedures and systems to ensure that personal information collected, stored or disclosed is up to date, accurate, complete and relevant. As part of this, if information is no longer required, then it should be destroyed or de-identified in accordance with the legal requirements. See also APP 11 in relation to this, below. Also ensure you meet the retention requirements for health-care records which are required to be kept for a minimum period. See APP 11 and also the EPA Code of Ethics and Conduct section 2.2 and Appendix 4.

Note: EPA recommends that you update/check the accuracy of your client records within a time frame that you deem reasonable and make it clear to clients that it is a requirement that they notify you of any changes to their personal information.

APP 11: Security of personal information

This section is also relevant to data protection and data storage

Health professionals must take reasonable steps to protect the personal information they hold from misuse, interference (including from computer attacks) or loss, and from unauthorised access, modification or disclosure. As of 1 February 2018, new legislative guidelines came into effect regarding increased care with Data Collection. A Guide to information security is available at http://www.oaic.gov.au/privacy/privacy- resources/privacy-guides/guide-to-information-security. Also see our separate document Data Protection Policy Guidelines for further information.

Notifiable Data Breach (NDB) scheme

The NDB scheme applies to all entities with existing personal information security obligations under the Privacy Act. The NDB scheme requires entities to notify affected individuals and the Australian Information Commissioner (Commissioner), in the event of an 'eligible data breach' [10 – Identifying eligible data breaches: https://bit.ly/2QbrII3]

A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. Entities must conduct a prompt and reasonable assessment if they suspect that they may have experienced an eligible data breach. [11 – Notifiable Data Breaches scheme: https://bit.ly/2Rt64Um]

AAPP 11 link ~ https://bit.ly/2epgi1w

Action Required:

Review your record storage practices, procedures and systems to ensure personal information is secure to prevent any of the above occurrences. Where required, introduce measures to protect against computer attacks, and review computer passwords on a regular basis. Read the EPA's Data Protection Policy to ensure you are up-to-date with all relevant procedures.

Health professionals are required to take reasonable steps to destroy or de-identify personal information if it is no longer needed for any authorised purpose, subject to exceptions such as any ethical requirements or any legal requirements which may differ from State to State.

Action Required:

Review your files on an annual basis to see if they may be destroyed once the ethical and legal requirements have been met. Refer to the EPA Code of Ethics and Conduct section 2.2 for retention of client records and Appendix 4 for disposal of records.

APP 12: Access to personal information

Health professionals must respond within a reasonable period when a client requests access to personal information. If Health professionals charge clients to gain access to information, the charge must not be excessive, and must not apply to lodging the request for access.

Health professionals may refuse clients access to their personal information if there is a serious threat to the life, health or safety of an individual or the public. Note that under the previous law (as with APP 6), the threat to life had to be imminent, but this is no longer the case.

Where there are grounds for refusing access, health professionals must provide in writing the reasons for the refusal and the mechanisms available to complain about the refusal (refer to APP 12.9). Health professionals need to also take steps to give access in a way that meets the needs of the client (APP 12.5), such as through an agreed intermediary (APP 12.6).

APP 12 link ~ https://bit.ly/2nga7Ty

Action Required:

Review your practices and procedures for responding to requests from clients for access to personal information (including timeframes for responding, how access is given, the provision of written reasons and any associated charges). It is suggested that you check whether a client's personal information is correct, and update this information accordingly.

The EPA recommends that no more than 30 days to respond to any request for access is acceptable practice.

APP 13: Correction of personal information

APP 13.1 requires that you 'take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.'

If health professionals correct a client's personal information that has previously been disclosed by them to another entity, they must take reasonable steps to notify the other entity of the correction if requested to by the client.

APP 13 link ~ https://www.oaic.gov.au/assets/privacy/app-guidelines/APP-Guidelines-Chapter-13-v1.1.pdf

Action Required:

Review your practices and procedures for responding to requests from clients for access to and correction of personal information (including timeframes for responding, how access is given, the provision of written reasons and any associated charges). It is suggested that you check whether a client's personal information is correct, and update this information accordingly. The EPA recommends that no more than 30 days to respond to a request for access is acceptable practice.

In addition to responding to requests by the client for correction, you should remind your clients to update you in the case that any of their details change, so that you can update their records. You can do this via a sign in your client waiting room, a sentence at the bottom of your initial consent form, or the like.

What happens if an APP is breached?

Breach of an APP in relation to personal information about an individual is known as "an interference with the privacy" of that individual. The meaning of this will be obvious to EPA members, due to the integrity of practice set and required under the EPA Code of Ethics and Conduct. An important premise of health-care is always to do no harm – this is both very basic and fundamental to taking the responsibility of being a health- care provider. How you treat your clients' personal information is part of this.

The Australian Information Commissioner has powers to investigate possible interferences with privacy, either following complaint by the individual concerned or on the Commissioner's own initiative. The Office of the Australian Information Commissioner (OAIC) will generally attempt to conciliate any complaint. However, where conciliation is not effective, the OAIC may use other tools, including determinations, enforceable undertakings, or in the case of serious or repeated breaches, initiating court proceedings for civil penalties.

Key current points applicable in relation to privacy are:

- One set of 13 Australian Privacy Principles (APPs) regulates the handling of personal information.
- The APPs apply to Australian Government agencies and businesses with a turnover of more than $3 million, as well as all private health service providers.
- Privacy policies must now include information for clients about making complaints about breach of privacy.
- Clients must be provided with the option to interact anonymously or by using a pseudonym, where this is requested and practical and legally allowable.
- Personal information can be disclosed if there is a threat to the life, health or safety of an individual or the public, but this threat no longer needs to be 'imminent'.
- Personal information can now be disclosed to assist in locating a missing person.

- Personal information that is stored electronically must be protected from computer attacks – including new data protection legislation effective 1 February 2018.
- Personal information must be destroyed or de-identified once it is no longer required for any ethical or legal purpose.
- Where grounds to refuse a request for access to information apply, reasons must be provided in writing as well as information about making a complaint, and steps must be taken to give access in a way that meets the client's needs.

All documentation developed by the EPA regarding Privacy Policy laws is a guide only and all practitioners are responsible for reading and applying the legislation as applicable to them. As a health-care practitioner, you are solely responsible for applying the principles of privacy law (and all other applicable laws and regulations) to your practice.

Further information

For further information refer to Privacy fact sheet 17: Australian Privacy Principles at Office of the Australian Information Commissioner: https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles