Australian Privacy Principle (APP)	OVERVIEW	AKA	MEMBER
APP 1- Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.	The AKA must have a relevant privacy principle that adequately explains the collection, use and management of personal information.	Practitioners in a position of collecting personal information must have a current privacy policy. This may be one that applies to all within a clinic or members may utilise AKA policy.
APP 2 – Anonymity and pseudonymity	Require APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.	This may be applicable but has a practicality test. Meaning it does not apply if ordered by law or if impracticable to deal with pseudonyms or unidentified individuals.	Generally it is impractical to deal with persons who will only identify themselves with a pseudonym. Exemptions apply for having to have this option available for clients due to the impractical nature.
APP 3- Collection of solicited personal information	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of "sensitive" Information.	You must ONLY collect information that is necessary or directly relates to one or more of the AKA's functions. Other than sensitive information, the AKA must not collect information unless reasonably necessary for its function. Sensitive information must be collected directly from the individual and only if the information relates to the AKA's function.	You must ONLY collect information that is necessary or directly relates to one or more of the business/practitioner's functions. Other than sensitive information, the practitioner must not collect information unless reasonably necessary for its function. Sensitive information must be collected directly from the individual and only if the information relates to practise.
APP 4- Dealing with unsolicited personal information	Outlines when APP entities must deal with unsolicited personal information.	The AKA may become aware of information from persons or about other persons. Where that information may be interesting it is not of business nature of the AKA and such information should not be noted or shared.	Unsolicited personal information may be necessary in practise. It may form part of client information. It must be kept only where it relates to the person's therapeutic goals.
APP 5- Notification of collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.	The AKA must state what personal information it is collecting about a person and if they are utilising other sources to collect this information.	Practitioners must seek approval from an individual to seek information about the individual from other practitioners.
APP 6- Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.	The AKA must seek approval or state by way of law how and who it shares personal information with.	Practitioners must seek approval from an individual to share information about the individual with other practitioners.
APP 7- Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.	The AKA must not use personal information for the purpose of direct marketing, unless, permission of the dividual has been obtained and the AKA provides an option to have personal information removed from direct marketing.	Practitioners must not use personal information for the purpose of direct marketing, unless, permission of the individual has been obtained and you provide an option for an individual to have their personal information removed from direct marketing. For example; you may collect mobile numbers and email addresses but unless you expressly request permission to use those for sending direct marketing, you may not. If permission is given, you must include an option to unsubscribe or opt out of the marketing and maintain these records.
APP 8- Cross border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before its disclosure overseas.	The AKA must be aware where personal information is stored. It must be stored where APP's are applied to the storage and transmission of personal information. This also applies to where an agency is used for that purpose. The AKA must have awareness of where Australian data is being stored and kept safe by the APPs.	A practitioner must be aware of where personal information is stored. It must be stored where APP's are applied to the storage and transmission of personal information. This applies to all record keeping in clinics.

APP 9- Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.	Government identifiers are not to be utilised for identification purposes.	Government identifiers are not to be utilised for identification purposes.
APP 10- Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of its use or disclosure.	The AKA must take reasonable steps to ensure personal information is kept updated.	Practitioners must take reasonable steps to ensure personal information is kept updated.
APP 11- Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.	The AKA must take steps to secure personal information. At the point in time the data is no longer required, for example at the end of membership, the information must be de-identified.	Practitioners must take steps to secure personal information.
APP 12- Access to personal information	Outlines an APP entity's obligation when an individual requests to be given access to personal information about them by the entity. This includes a requirement to provide access unless a specific exemption applies.	The AKA must be able to efficiently provide its members with access to personal information contained about them.	Practitioners must be able to efficiently provide individuals with access to personal information contained about them.
APP 13- Correction of personal information	Outlines an APP entity's obligation in relation to correcting the personal information it holds about individuals.	The AKA must take steps to correctly update any information it finds to be incorrect.	Practitioners must take steps to correctly update any information they find to be incorrect about their clients.