Avant – Guide To Privacy Reforms
Guide to privacy reforms checklist

Avant Mutual Group Limited
ABN 58 123 154 898

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
There are some changes to what constitutes 'personal information' and 'sensitive information' under the Privacy Act.	**Section 6** of the Privacy Act	Do we handle 'personal information' or 'sensitive information'? Most health information will be sensitive information: • Medical information • Personal details – contact details, Medicare number • Biological samples that can be linked to medical notes • xrays	Review information held by your organisation to determine whether and what 'personal information' or 'sensitive information' is handled. If 'yes', you must ensure that APPs are complied with		
APP entities must take reasonable steps to implement new practices, procedures and systems that will ensure compliance with the new APPs and any registered APP Codes. This may include training staff or establishing procedures to identify and manage privacy risks.	**APP 1 –** Open and transparent management of personal information	What reasonable steps do we need to take to implement new practices, procedures and systems that will ensure compliance with the new APPs and any registered APP Codes?	Review current practices, procedures and systems to determine what needs to be done to ensure compliance with the new APPs and any registered APP Codes. **Working through the actions in the rest of this checklist will assist APP entities to meet their obligations under this APP.**		
APP entities should have an up to date APP privacy policy that is reviewed regularly. The new laws set out some requirements for privacy policies, including requirements for content and availability.	**APP 1 –** Open and transparent management of personal information	Do we have a privacy policy? If so, is it up to date? Does it cover the matters listed in APP 1.4? Is it freely available?	Review or draft APP privacy policy (see Template). Make APP privacy policy available in an appropriate form and for free. For example, on the practice's website or on a notice board in the waiting room.		
APP entities must take reasonable steps to implement new practices, procedures and systems that will ensure the APP entity can handle privacy inquiries and complaints from individuals.	**APP 1 –** Open and transparent management of personal information	What reasonable steps do we need to take to ensure we have practices, procedures and systems in place for handling privacy inquiries and complaints?	Review practices, procedures and systems for handling privacy inquiries and complaints within the practice. Have a designated staff member in the practice responsible for receiving and responding to complaints.		

Telephone 1800 128 268 **Email** memberservices@avant.org.au **www.avant.org.au**

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
APP entities must give individuals the option to interact with their APP entity anonymously or by using a pseudonym. You may not have to do this if an exception applies in relation to a particular matter.	**APP 2 –** Anonymity and pseudonymity	The legal requirements to maintain medical records of consultations will usually make it difficult for practices to allow patients to interact with the practice anonymously or by using a pseudonym.	Obtain advice if a patient seeks to rely on APP2 and wishes to obtain health care on an anonymous basis.		
There are new rules that apply to collection practices and notices when collecting personal information and/or sensitive information (such as health information). These rules include proscriptive requirements about the content of notices.	**APP 3 –** Collection of personal and sensitive information **APP 5 –** Notification of collection	Do we collect personal and/or sensitive information? Do we ensure that sensitive information is collected in accordance with the higher protections in APP 3.3? How and what matters do we notify individuals about when collecting their personal or sensitive information?	Review collection practices, procedures and systems, including collection notices. Ensure the privacy policy covers the necessary collection notices. (*see Template*)		
There are new rules on how to deal with unsolicited personal information, including when this information must be destroyed or de-identified.	**APP 4 –** Dealing with unsolicited personal information	Do we receive unsolicited personal information? What are our practices, procedures and systems for dealing with unsolicited information? Who is responsible in the practice for making decisions about this type of information?	Review practices, procedures and systems for dealing with unsolicited information. Unsolicited information can be retained if it could have been lawfully collected and used, otherwise it should be destroyed or de-identified.		
There are new rules on when personal information and sensitive information can be used or disclosed.	**APP 6 –** Use or disclosure	For what purposes do we use and disclose personal information and sensitive information?	Review practices, procedures and systems for the use and disclosure of personal information and sensitive information.		
There are new rules on when personal information can be used or disclosed for the purpose of direct marketing. These rules primarily apply to organisations, but could apply to agencies in some circumstances.	**APP 7 –** Direct marketing	Does APP 7 apply to us? If so we, or do we want to, use or disclose personal information for the purpose of direct marketing? Do we meet any of the exceptions in APP 7 that permit us to do so?	Review direct marketing practices, procedures and systems (including whether individuals are provided with an easy way to opt out of receiving direct marketing).		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
There are new rules about an APP entity's accountability for personal information that it has disclosed to overseas recipients.	**APP 8 –** Cross border disclosure	Do we send personal information overseas? Do we have appropriate arrangements with overseas recipients to ensure that personal information that is disclosed overseas is handled in accordance with the APPs?	Review practices, procedures and systems for sending personal information overseas (this may include reviewing outsourcing agreements or checking with cloud server providers).		
There are new exceptions to the general prohibition against the adoption, use or disclosure of government related identifiers by organisations. In some circumstances, APP 9 will apply to agencies.	**APP 9 –** Adoption, use or disclosure of government related identifiers	Does APP 9 apply to us? If so, do we collect government related identifiers? Are we permitted to adopt, use or disclose government related identifiers under the new exceptions?	Review practices, procedures and systems for the adoption, use or disclosure of government related identifiers. Review the systems in place for the use of PCEHR identifiers.		
APP entities must take reasonable steps to ensure that the personal information that they collect, use or disclose is up to date, complete and accurate (personal information used or disclosed must also be relevant, having regard to the purpose of the use or disclosure)	**APP 10 –** Quality	What reasonable steps do we need to take to ensure that the personal information we collect, use or disclose is up to date, complete and accurate and relevant for the purpose of the use or disclosure?	Review practices, procedures and systems for ensuring personal information collected, used or disclosed is up to date, complete and accurate and relevant for the purpose of the use or disclosure.		
APP entities must take reasonable steps to protect the personal information they hold from misuse, interference (this may include introducing measures to protect against computer attacks), loss and from unauthorised access, modification or disclosure	**APP 11 –** Security	What reasonable steps do we need to take to ensure that the personal information we collect is protected from: • misuse, • interference, • loss and • unauthorised access, modification or disclosure?	Review practices, procedures and systems for ensuring personal information is protected from misuse, interference, loss and from unauthorised access, modification or disclosure (refer to the OAIC's Guide to information security and also the RACGP's Information and Security Standards 2013).		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
APP entities 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 some exceptions	**APP 11 –** Security	What reasonable steps do we need to take to ensure personal information is destroyed or de-identified when it is no longer needed for any authorised purpose? Do any exceptions apply to the information we hold?	Review practices, procedures and systems for ensuring personal information is destroyed or de-identified when it is no longer required by law to be kept.		
There are new rules on how APP entities are to respond to requests for access to and correction of personal information (including timeframes, the manner in which access is to be given, when written reasons are required and charging). There is also a new rule about when an APP entity should correct personal information, even if it has not received a request from an individual.	**APP 12 –** Access **APP 13 –** Correction	What are our processes for responding to requests from individuals for request for access to and correction of personal information? What are our processes for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?	Review practices, procedures and systems for: • correcting personal information and/or • responding to requests from individuals for access to and • correction of personal information (including timeframes for responding, the manner in which access is given, the provision of written reasons and charges for access and correction). • A designated staff member should be responsible for co-ordinating such requests.		

This Checklist is based on a Checklist created and published by the Office of the Information Commissioner: Privacy business resource 2: Privacy Act reforms – Checklist for APP entities (organisations) *Office of the Australian Information Commissioner website* – www.oaic.gov.au. **Changes have been made to the Checklist to adapt it for use in medical practices.**

XXXX/02-14