Addendum 1 – Compliance indicators for the Australian Privacy Principles

The compliance indicators for the Australian Privacy Principles (APP) matrix identify the specific actions that comprise essential privacy practices. This document is designed to assist general practice to meet its legal obligations of the APP, by providing a brief explanation of each APP requirement and the steps general practice need to take to ensure compliance.

It is assumed the practice will provide appropriate education and training to facilitate compliance with these privacy practices.

The compliance indicators at level 3 reflect the minimum level required to comply with the APP.
The compliance indicators for higher levels provide the basis for incremental privacy accountability and practice improvement.

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Part 1: Consideration of personal information privacy **Australian Privacy Principle 1: Open and transparent management of personal information**					
Reasonable steps (APP 1.2)	APP review and compliance not undertaken	APP review partially undertaken	The practice has documented and implemented procedures to meet the APP The practice has undertaken an assessment against these compliance indicators	The practice has documented and implemented procedures to meet the APP Staff trained in awareness and implementation	The practice has documented and implemented procedures to meet the APP Staff trained in awareness and implementation annually
APP Privacy Policy content (APP 1.3)	No APP Privacy Policy	Incomplete APP Privacy Policy	The practice has a written APP Privacy Policy that includes the content specified in APP 1.4 (refer to *The Privacy Handbook* and APP Privacy Policy template) This policy is available publicly however the (internal) practice operational privacy policy is not required to be made public	The practice has a written APP Privacy Policy that includes the content specified in APP 1.4 (refer to *The Privacy Handbook* and APP Privacy Policy template) Periodically reviewed	The practice has a written APP Privacy Policy that includes the content specified in APP 1.4 (refer to *The Privacy Handbook* and APP Privacy Policy template) Reviewed annually
Availability of APP Privacy Policy (APP 1.5)	No APP Privacy Policy available	The practice APP Privacy Policy available on request only	The APP Privacy Policy is accessible on the practice website or in printed format	The APP Privacy Policy is accessible on the practice website or printed format on request, provided free of charge	The APP Privacy Policy is accessible on the practice website and in printed or electronic format upon request, provided free of charge

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Process for privacy inquiries or complaints (APP 1.2)	No formal procedure for handling inquiries and complaints	No written procedure for handling inquiries and complaints	The practice has a written procedure for handling inquiries and complaints	The practice has a written procedure for handling inquiries and complaints Procedure freely available on website	The practice has a written procedure for handling inquiries and complaints Procedure available on website and in other formats upon request Staff trained in these procedures
Australian Privacy Principle 2: Anonymity and pseudonymity					
Option for patients to have anonymity or use a pseudonym, where practicable (APP 2.1 & 2.2)	No facility to handle anonymity or pseudonymity	Process in place for anonymity or pseudonymity in exceptional circumstances only	The practice has processes in place (manual or electronic) to handle requests for anonymity or pseudonymity *Note: This is for when patients do not wish to identify themselves (anonymity) and do not want information that can identify them to be recorded. Pseudonymity is used when a patient does not want to have their real identity recorded or readily accessible, for instance if the patient is publicly well known. In the case of pseudonymity, it may still be possible to link information to their real identity*	The practice has processes in place (manual or electronic) to handle requests for anonymity or pseudonymity The practice computer system is capable of handling anonymity or pseudonymity	The practice has processes in place (manual or electronic) to handle requests for anonymity or pseudonymity The practice computer system is capable of handling anonymity and pseudonymity Staff trained in procedures
Part 2: Collection of personal information **Australian Privacy Principle 3: Collection of solicited personal information**					
Collection of personal information other than sensitive information (APP 3.1 & 3.2)	No process for deciding what personal information should or should not be collected	Ad hoc decisions are made on how, what and when personal information is collected	The practice has documentation on how, what and when personal information is collected	The practice has documentation on how, what and when personal information is collected Processes amended with all new personal information collection requests	Written policy on how, what and when personal information is collected, and notification of collection Policy amended with all new or revised personal information collection requests Policy reviewed annually Staff trained in policy

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Collection of sensitive information consent (APP 3.3 & 3.4)	Patient consent is not considered or is assumed	Patient consent is assumed. No formal policy and guidance for consent documented	The practice follows appropriate policy on all levels of consent required, and how this is obtained and recorded	The practice follows written policy explaining all levels of consent required, and how this is obtained and recorded Staff trained in consent requirements	The practice follows written policy explaining all levels of consent required, and how this is obtained and recorded Staff trained annually on consent requirements Documented consent reviewed yearly (audited)
Means of collection (APP 3.5 & 3.6)	Requirement for authorisation for the collection of information from someone other than the patient is not known	Authorisation for the collection of information from someone other than the patient is not usually obtained	The practice only collects information directly from the patient, unless there is authorisation for collection from someone else Staff aware of requirement	The practice only collects information directly from the patient, unless there is authorisation for collection from someone else Staff trained in requirement	The practice only collects information directly from the patient, unless there is authorisation for collection from someone else Written policy on collection Staff trained on policy
Australian Privacy Principle 4: Dealing with unsolicited personal information					
Personal information received but not collected by the practice originally (APP 4.1, 4.2, 4.3 & 4.4)	No process identifying or managing unsolicited personal information	Ad hoc decisions on unsolicited personal information identification and management	The practice evaluates all information it receives that it did not request (unsolicited information) to decide if it should be kept, acted on or destroyed	The practice evaluates all information it receives that it did not request (unsolicited information) to decide if it should be kept, acted on or destroyed. The practice has written procedures for identification, management and evaluation of unsolicited information Staff aware of procedures	The practice evaluates all information it receives that it did not request (unsolicited information) to decide if it should be kept, acted on or destroyed. The practice has written procedures for identification, management, and evaluation of unsolicited information, including secure destruction and de-identification Procedures reviewed annually Staff trained in procedures

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Australian Privacy Principle 5: Notification of the collection of personal information					
Notification to patient of information collected (APP 5.1 & 5.2)	No process for notification to patients when the practice receives or collects personal information it did not request	Ad hoc decisions made on notification to patients when the practice receives or collects personal information that it did not request	When the practice collects or receives personal information that the patient is not aware of, the practice notifies the patient of this collection. The notification must include the reason for collecting it, what the practice will do with the information and who else the practice might share this with (potential further disclosure to third parties). See *The Privacy Handbook* and APP Privacy Policy template for further information	The practice has documented procedures for notification to patients of unsolicited personal information Notifications include all APP 5.2 stipulations Policy amended when information processes altered	The practice has written policy and procedures for notifying patients of unsolicited personal information collection. Notifications include all APP 5.2 stipulations Policy reviewed annually and when personal information processes altered Staff trained in policy
Part 3: Dealing with personal information **Australian Privacy Principle 6: Use or disclosure of personal information**					
Use or disclosure (secondary use) (APP 6.1, 6.2 & 6.3)	No policy or process in place for assessing the need for obtaining consent for secondary use of personal information	Ad hoc decisions made on the circumstances where patient consent is required for secondary use of personal information	The practice obtains consent from the patient for the secondary use of their information in cases it would not be reasonable for the patient to expect their information to be used for this purpose, or where the information is not de-identified Secondary uses of data are recorded *Note: If the patient would normally expect the practice to use their information for a secondary purpose and this information is de-identified then consent is not required* All disclosures recorded (compliance with RACGP Data Governance Principles)	The practice obtains consent from the patient for the secondary use of their information in cases it would not be reasonable for the patient to expect their information to be used for this purpose, or where the information is not de-identified. Patient consent is documented Secondary uses of data are recorded The de-identification process is checked Records of the secondary use are reviewed (refer to the RACGP Data Governance Principles)	The practice refers to and documents compliance with the RACGP Data Governance Principles for each instance of secondary use. This includes written policy on secondary use of information Staff trained in policy Disclosure records audited periodically

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Australian Privacy Principle 7: Direct marketing					
Information to be used for direct marketing (APP 7.1-7.8)	No procedures in place or consideration of information for direct marketing	Consideration of use and disclosure of information for direct marketing. No policy or procedures in place	The practice does not engage in direct marketing; or If the practice does engage in direct marketing then the practice has procedures for individual consent and recording of this consent. In addition, a simple process for patients to request not to receive direct marketing is in place	The practice does not engage in direct marketing or written procedures for the use of information for direct marketing, consent and opt-out process are in place Staff aware of these procedures	The practice does not engage in direct marketing or written policy and procedures for the use of information for direct marketing, consent and opt-out process are in place Procedures to obtain retrospective consent from existing patients are in place Staff trained in policy
Australian Privacy Principle 8: Cross-border disclosure of personal information					
Information sent or disclosure to overseas recipient (APP 8.1 & 8.2) *Note: this includes recordings sent overseas for transcription and image for reporting*	No process for overseas disclosure of information	Ad hoc decisions on overseas disclosure No written procedure or policy on overseas disclosure arrangements Consent not obtained	The practice has a procedure that ensures any overseas recipient of information has substantially similar protection to Australian Privacy Principles and consent has been obtained for disclosure of this information where required (see APP 8.3 for exceptions)	Procedure (as per level 3) documented Audit of all information sent overseas and procedure for assessing similar protection undertaken Staff aware of procedures	Written policy and documented process procedure for overseas disclosure Procedure for ensuring APP comparability documented and audited Staff trained in policy
Australian Privacy Principle 9: Adoption, use and disclosure of government related identifiers					
Use of Individual Health identifier (IHI) (APP 9.1, 9.2 & 9.3)	No process for adoption, use and disclosure of Individual Health Identifier (IHI) considered by practice	Ad hoc decisions made on the use of IHIs and other government identifiers (such as the Medicare number) in the practice computer systems	The practice does not use the IHI or any other government identifier such as the Medicare number, as the primary patient identifier in the practice computer systems	The practice does not use the IHI or any other government identifier such as the Medicare number, as the primary patient key in the practice computer systems Procedures for correct handling and management of IHIs relevant to the practice developed Compliance with RACGP *Computer and information security standards*, Standard 12.4 Level 4	The practice does not use the IHI or any other government identifier such as the Medicare number, as the primary patient key in the practice computer systems Written policy on IHI use in practice in addition to IHI legislation Compliance with RACGP *Computer and information security standards*; Standard 12.4 Level 5 Staff trained in policy

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Part 4: Integrity of personal information **Australian Privacy Principle 10: Quality of personal information**					
Personal information is accurate, up-to-date and complete. (APP 10.2 & 10.2)	No procedures in place to ensure accuracy, currency and completeness of personal information	Ad hoc procedures used to ensure accuracy, currency and completeness of personal information	The practice has a process for ensuring personal information is accurate, up-to-date and complete during data collection, and when information is used or disclosed	The practice has documented procedures for ensuring personal information is accurate, up-to-date and complete during data collection, and when information is used or disclosed Staff aware of procedures	Written policy on personal information quality at data collection, use and disclosure, including periodic audit and review Staff trained in policy
Australian Privacy Principle 11: Security of personal information					
Protection of information (APP 11.1)	No formal processes for security protection	Partial compliance with RACGP *Computer and information security standards* at minimum acceptable level for each Standard	Demonstrated compliance with RACGP *Computer and information security standards* at minimum acceptable level for each Standard	Documented compliance with RACGP *Computer and information security standards* at minimum acceptable level for each Standard	Documented compliance with RACGP *Computer and information security standards* above minimum acceptable level for each Standard
Secure disposal of information (APP 11.2)	No formal process for secure disposal of information	Partial compliance with RACGP *Computer and information security standards*, i.e. below Level 4 for Standard 11.5 OR no procedures for secure destruction or de-identification of an individual's information	Demonstrated compliance with RACGP *Computer and information security standards*, Standard 11.5 Level 4 and personal information no longer required to be kept by the practice must be securely destroyed or permanently de-identified	Demonstrated compliance with RACGP *Computer and information security standards*, Standard 11.5 Level 4 and personal information no longer required to be kept by the practice must be securely destroyed or permanently de-identified Disposal and de-identification of patient information recorded	Demonstrated compliance with RACGP *Computer and information security standards*, Standard 11.5 Level 4 and personal information no longer required to be kept by the practice must be securely destroyed or permanently de-identified Disposal and de-identification recorded and audited Staff trained in secure disposal and de-identification policy

			Minimum		
Compliance Indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**	**Level 4 Managed**	**Level 5 Optimised**
Part 5: Access to, and correction of, personal information **Australian Privacy Principle 12: Access to personal information**					
Access by individual to their personal information (APP 12.1-12.10)	No procedure for individuals' access to their personal information	Ad hoc procedures initiated when requested	The practice has a procedure for dealing with requests for access to personal information. This is provided in the format requested where possible. If the practice refuses this request, the practice informs the patient in writing of the reasons for the refusal (For charges and time frames refer to *The Privacy Handbook*)	The practice has a documented procedure for dealing with requests for access to personal information. This is provided in the format requested where possible. If the practice refuses this request, the practice informs the patient in writing of the reasons for the refusal The documented procedures include exceptions procedures, charges and time frames	Written policy and procedure for patient access to their information. This will include exceptions for refusal, charges and time frames Accessed recorded and reviewed periodically Staff trained in policy
Australian Privacy Principle 13: Correction of personal information					
Correction (APP 12.1-12.10)	No procedure for correction of personal information at a patient's request	Ad hoc procedures for correcting personal information only initiated when requested	The practice has a procedure for correcting personal information. This includes notification to third parties; written refusal to correct notification; provision for individual's statement of inaccuracy to be associated with that information; and no charge may be made for the correction	Documented procedure for correcting personal information including refusal procedures and time frames	Written policy and procedure for correcting personal information. This will include refusal, inaccuracy statements and time frames Corrections recorded and reviewed periodically Staff trained in policy

The information in this table was adapted and reproduced with permission from Dr Patricia Williams

Disclaimer

Published by The Royal Australian College of General Practitioners, 100 Wellington Parade, East Melbourne VIC 3002 Australia. Tel 03 8699 0414, Fax 03 8699 0400, www.racgp.org.au

Published February 2014. © The Royal Australian College of General Practitioners.

RACGP