Avant – Guide to Privacy Reforms

Avant
mutual group

Contents

Chapter 1: Overview of privacy legislation

Introduction

The Privacy Act 1988 (Cth)

The Commonwealth Privacy Act came into force in 1988. It was extended to the private sector in December 2001. It applies to all **health service organisations** regardless of their turnover. Outside the health sector the Act only applies to private organisations with an annual turnover in excess of $3m.

The Act regulates the **collection, use and disclosure** of personal information from which an individual can be identified. However, it does not apply to information held by an employer about its current or former employees making up part of their employment records.

Most of the information collected and used by health practices will be considered as "sensitive information" and subject to more stringent protection under the Act.

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 commences on 12 March 2014

From this date the existing 10 National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs) will be replaced by a single set of 13 Australian Privacy Principles (APPs). They will apply to the public and private sector entities covered by the Act – "APP entities" (*see summary*).

APP entities will need to have an up to date and documented "privacy policy" that includes specific information (*see template privacy policy*).They must also have practices, policies and procedures in place to ensure compliance with the APPs (*see checklist*).

A new section (16A&B) outlines a number of "permitted" situations for the collection, use, and disclosure of health information (*see summary*).

If health information is being sent and stored overseas by a practice it will have to comply with the requirements in APP 8 (*see checklist*).

Enhanced powers and penalties

There are new, enhanced penalties and investigatory powers under the Act. The Privacy Commissioner has the power to conduct privacy assessments or investigations. There is a civil penalty of up to **$1.7m** for corporations and **$340,000** for individuals.

The penalty provisions may apply if a practice:

- Does an act or engages in a practice that is a **serious interference with the privacy** of an individual; or
- The practice repeatedly does an act or engages in a practice that is **an interference in the privacy** of one or more individuals.

The Privacy Commissioner has to apply to the Court for a monetary penalty to be imposed, and the Court can impose penalties it considers appropriate taking into account:

- The nature and extent of the contravention and any loss suffered.
- The circumstances in which the contravention occurred.
- Whether the practice/practitioner has previously been found by the Court to have engaged in similar conduct.

A **serious interference with the privacy** of an individual is not defined, but some examples given by the Privacy Commissioner are:

- Knowingly disclosing detailed and sensitive personal information held by a health services provider to a marketing organisation for direct marketing.
- Hacking of computer systems where the entity has not taken reasonable precautions to prevent or minimize the risk of hacking.

Mandatory Breach Notification Bill

The Commonwealth Government introduced a Mandatory Breach Notification Bill to Parliament in 2013 that has now lapsed. If that Bill is re-introduced and passed by Parliament it will create a mandatory obligation on practices to inform patients and the Privacy Commissioner of any serious privacy breaches.

Australian Privacy Principles	
APP 1	open and transparent management of personal information
APP 2	anonymity and pseudonymity
APP 3	collection of solicited personal information
APP 4	dealing with unsolicited personal information
APP 5	notification of the collection of personal information
APP 6	use or disclosure of personal information
APP 7	direct marketing
APP 8	cross-border disclosure of personal information
APP 9	adoption, use or disclosure of government related identifiers
APP 10	quality of personal information
APP 11	security of personal information
APP 12	access to personal information
APP 13	correction of personal information

State and Territory Privacy Legislation

Health service organisations are also bound by State and Territory privacy legislation (*see list of relevant legislation*). While there are similarities with the Commonwealth legislation it is important to seek advice if you are unclear about what law to follow.

The Commonwealth Privacy Act does not apply to the health information of **deceased persons** and disclosure of this information is regulated by state or territory legislation or the common law.

Requests for Access to Medical Records

- Patients have a right to request access to their medical records without providing a reason (but you can ask to clarify the scope of access).
- Access can only be refused on limited grounds:
  - pose a serious threat to life / safety
  - unreasonable impact on privacy of others
  - unlawful to disclose information
  - information is subject to legal privilege
- Access must be provided within specified timeframes.
- Administrative costs may be charged but they must be reasonable and not excessive.

State and Territory Legislation
For the private sector: Health Records and Information Privacy Act 2001 (NSW) Health Records Act 2001 (Vic) Health Records (Privacy and Access) Act 1997 (ACT)
For the public sector: Privacy and Personal Information Protection Act 1998 (NSW) Health Records Act 2001 (Vic) Information Privacy Act 2009 (Qld) Health Records (Privacy and Access) Act 1997 (ACT) Personal Information Protection Act 2004 (Tas) Information Act 2002 (NT) Administrative Policy based on Information Privacy Principles (4 Feb 2013)

Please contact Avant's Medico-Legal Advisory Service if you require advice about the use or disclosure of deceased patients' records and the application of State / Territory privacy legislation.

Summary of key Australian Privacy Principles Application to health practices

APP 1 Open and transparent management of personal information

The practice must have a **Privacy Policy** that covers specified information. Reasonable steps must be taken to make the Privacy Policy available to patients free of charge.

See: Privacy Policy

APP 3 Collection of solicited information

Sensitive information must only be collected if it is "reasonably necessary" for the operations of the practice, that is the provision of health services.

The collection has to be with the consent of the patient or his or her authorised representative (eg. parent or guardian).

The information should be collected from a patient personally unless it is not practicable or reasonable to do so.

Example: *information about a family member is obtained while taking a history from a patient. This is acceptable if the information is reasonably necessary to treat the patient.*

APP 5 Notification of collection

The practice must provide information to patients on its processes for:

- Accessing and correcting medical records
- Making and handling privacy complaints
- The location of any likely overseas recipients of information

This information can be included in the **Privacy Policy**.

APP 6 Use and disclosure of personal information

The practice can only use or disclose personal information for a "primary purpose" or a "secondary purpose".

A **"primary purpose"** is the particular purpose for which the information was collected. The Information Commissioner's Guidelines state that this purpose should be narrowly construed so patients understand how their information will be used.

Example: *a 12 week pregnant patient has blood tests to check her iron levels. The primary purpose of the collection of the blood test results is for treatment of the patient during her pregnancy.*

A **"secondary purpose"** can arise in these circumstances:

- **Consent –** a patient consents to the secondary use. This consent can be express or implied, but the patient must have capacity to give consent. The consent must also be informed and current.

- **Reasonable expectation of patients that information will be used or disclosed for a different purpose closely related to the primary purpose.** The "secondary purpose" is directly or closely related to the "primary purpose".

  Example: *the practice provides the patient's blood test results to her obstetrician. The patient would reasonably expect that her GP and obstetrician would share such information.*

- **Disclosure is required or authorised by law. Examples:**
  - Warrant from Police to access medical records
  - Subpoena to produce documents or give evidence
  - Mandatory notification of child abuse or notifiable diseases

- **There is a "permitted general situation" – 7 situations when personal information can be disclosed for a "secondary purpose" (section 16A). The 5 situations relevant to health practices are:**
  - **Health and Safety –** the practice has a reasonable belief that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety and it is unreasonable or impracticable to obtain consent from a patient. There is no longer a requirement that the threat is "imminent", but it must still be serious.
  - **Unlawful activity/serious misconduct –** the practice has a good reason to suspect that unlawful activity or misconduct of a serious nature that relates to the practice's functions has been, or is being or may be engaged in and the use or disclosure of information is necessary for the practice to be able to take appropriate action.

    Example: *a pharmacist thinks that prescriptions have been forged by a staff member.*
  - **Location of a missing person –** the practice has a reasonable belief that the use or disclosure of personal information is reasonably necessary to locate a person who has been missing.

    Example: *medical records indicate that 16 year old patient who has been reported missing was proposing to travel interstate to visit a person she had met via Facebook.*
  - **Defending or establishing a legal or equitable claim –** this is a new provision that confirms the right of practices to disclose information to respond to complaints or claims.

    Example: *disclosure of a patient's medical records to an insurer in order to seek assistance to respond to a disciplinary complaint.*
  - **Confidential mediation / ADR processes –** this is another new provision that confirms the right of practices to use or disclose personal information during a confidential alternative dispute process such as a mediation.

- **There is a "permitted health situation" – 3 additional situations when a practice can use or disclose health or genetic information for a "secondary purpose" are:**
  - **Research –** if it is relevant to public health or safety, it is impracticable to obtain a patient's consent, conducted in accordance with research guidelines and once disclosed the information will not be disclosed by the recipient.

- **Prevention of serious threat to life, safety or health of a genetic relative.**

  Example: *a patient with a rare genetic disease has dementia and her children request access to her medical records to ascertain the nature of her disease.*

- **Responsible person/Guardian –** where a patient is either physically or mentally incapable of giving consent, a practice may disclose information to a responsible person or guardian where the disclosure is necessary to provide appropriate care or treatment to the patient or for "compassionate reasons". The disclosure must not be contrary to any wishes expressed by the patient when they had capacity. It must also be limited to the extent that is reasonable and necessary for providing appropriate care or fulfilling the compassionate reasons.

  Examples: *(a) a patient has been discharged from hospital and the guardian requests details of the medications the patient requires to ensure the patient receives the necessary treatment (b) a patient has been admitted to hospital in an unconscious state and his carer is provided details of his condition on "compassionate grounds".*

APP 7 Direct marketing

The practice must not use or disclose sensitive information for the purpose of direct marketing unless the individual consents to the use or disclosure for that purpose.

Direct marketing involves the use of personal information to communicate with an individual to promote goods and services.

Example: *sending a brochure in the mail directly to a patient about services offered at the practice, or sending an SMS to a patient about health-related services available at the practice.*

Individuals must be made aware of how to opt out and the practice must comply with a request to opt out.

APP 8 Cross border disclosure of personal information

If the practice is going to send personal information overseas, before doing so it must take reasonable steps to ensure that the overseas recipient does not breach the APPs.

Example: *having a contract with an overseas cloud service provider that requires them to comply with the APPs.*

There are exceptions to this including:

- where the overseas recipient is subject to a similar law or binding scheme with protections substantially similar to the APPs, and there is a mechanism for an individual to enforce the protections provided by that law or scheme or
- the individual consents after being expressly informed that information will be sent overseas

APP 9 Use of government identifiers

The practice must not adopt, use or disclose a government related identifier unless:

- the adoption, use or disclosure is required or authorised by law
- it is reasonably necessary to verify the identity of the individual

- it is reasonably necessary to fulfill obligations to a Commonwealth agency or state or territory authority
- the practice reasonably believes it is necessary to lessen or prevent a serious threat to the life, health and safety of an individual or to public health and safety
- the practice reasonably believes that use or disclosure is necessary for the practice to take action in relation to suspected unlawful activity or misconduct of a serious nature
- the practice reasonably believes that the use or disclosure is reasonably necessary for enforcement related activities of an enforcement body.

A government related identifier includes a Medicare number, drivers licence number, passport number and Centrelink reference number.

Example: the practice uses patients' Medicare numbers as the basis for its patient identification system. This is not permitted, however the practice could use a patient's Medicare number, including physically viewing the patient's Medicare card, along with other data, to check the identity of the patient for treatment and billing purposes if there is a concern about fraud or identity theft.

An individual cannot consent to the adoption, use or disclosure of a government related identifier if it is not otherwise permitted.

APP 10 Quality of personal information

The practice must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. **Compliance tip:** *contact details for patients should be regularly checked with patients to ensure they are up to date and accurate.*

There is a new requirement that information also be "relevant" when it is used or disclosed.

APP 11 Security of personal information

The practice must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification and disclosure. There is a new requirement that practices also protect personal information from "interference". **Compliance tip:** *passwords are required by staff to access the practice's medical records system and they are changed on a regular basis.*

The practice is also now required to take reasonable steps to destroy or de-identify personal information that is no longer required for authorised purposes. However, this requirement will always be subject to any laws concerning the need to retain medical records.

APP 12 Access to personal information

Patients are entitled to request access to their health information and access must be provided unless an exception applies (see APP 6 above). If access is refused, the practice has to explain in writing why access is refused and how patients can complain about this decision.

There is a new requirement for practices to respond to patient requests for access within a "reasonable period". This is not defined in the Act, but in NSW it is specified as being within 45 days.

The practice can charge patients for providing access to medical records, but the fee cannot be "excessive". The AMA provides a guide to suggested fees.

APP 13 Correction of personal information

There is a new requirement for practices to take reasonable steps to correct personal information to ensure that it is up to date, relevant and not misleading.

The practice also has to notify other health organisations of any corrections made to information that may have been provided to them by the practice.

Where a patient requests a change to be made to his or her medical records, the practice must acknowledge the request within a reasonable time.

No charge can be made for the practice making the requested changes to the medical records.

Chapter 2: Checklist and template documents

Guide to privacy reforms checklist

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.**		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
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.		
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.		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
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 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.		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
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).		
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.		

The change	Relevant part of the Privacy Act	Consider	Action	Who?	Complete?
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.**

Privacy policy

Requirement for a privacy policy

A practice must have a clearly expressed and up to date policy about the management of personal information it holds.

Content of a privacy policy

The privacy policy must contain the following information:

a. the kinds of personal information that the practice collects and holds

b. how the practice collects and holds personal information

c. the purposes for which the practice collects, holds, uses and discloses personal information

d. how an individual may access personal information about the individual that is held by the practice and seek the correction of such information

e. how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the practice, and how the practice will deal with such a complaint

f. whether the practice is likely to disclose personal information to overseas recipients

g. if the practice is likely to disclose personal information to overseas recipients – the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of a privacy policy

A practice must take reasonable steps to make its APP privacy policy available:

a. free of charge and

b. in such form as is appropriate.

A practice will usually make its APP privacy policy available on its website or in the waiting area. If a person or body requests a copy of the APP privacy policy in a particular form, the practice must take reasonable steps to give the person or body a copy in that form for example, in soft copy or hard copy, by post or email.

APP Privacy Policy – Template

[to be modified to fit the needs of your practice]

Introduction

We are committed to protecting the privacy of patient information and to handling your personal information in a responsible manner in accordance with the Privacy Act 1988 (Cth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles and relevant State and Territory privacy legislation (referred to as privacy legislation).

This Privacy Policy explains how we collect, use and disclose your personal information, how you may access that information and how you may seek the correction of any information. It also explains how you may make a complaint about a breach of privacy legislation.

This Privacy Policy is current from **[insert 2014]**. From time to time we may make changes to our policy, processes and systems in relation to how we handle your personal information. We will update this Privacy Policy to reflect any changes. Those changes will be available on our website and in the practice.

Collection

We collect information that is necessary and relevant to provide you with medical care and treatment, and manage our medical practice. This information may include your name, address, date of birth, gender, health information, family history, credit card and direct debit details and contact details. This information may be stored on our computer medical records system and/or in hand written medical records.

Wherever practicable we will only collect information from you personally. However, we may also need to collect information from other sources such as treating specialists, radiologists, pathologists, hospitals and other health care providers.

We collect information in various ways, such as over the phone or in writing, in person in our **[insert clinic/practice/centre/rooms]** or over the internet if you transact with us online. This information may be collected by medical and non-medical staff.

In emergency situations we may also need to collect information from your relatives or friends.

We may be required by law to retain medical records for certain periods of time depending on your age at the time we provide services.

Use and Disclosure

We will treat your personal information as strictly private and confidential. We will only use or disclose it for purposes directly related to your care and treatment, or in ways that you would reasonably expect that we may use it for your ongoing care and treatment. For example, the disclosure of blood test results to your specialist or requests for x-rays.

There are circumstances where we may be permitted or required by law to disclose your personal information to third parties. For example, to Medicare, Police, insurers, solicitors, government regulatory bodies, tribunals, courts of law, hospitals, or debt collection agents. We may also from time to time provide statistical data to third parties for research purposes.

We may disclose information about you to outside contractors to carry out activities on our behalf, such as an IT service provider, solicitor or debt collection agent. We impose security and confidentiality requirements on how they handle your personal information. Outside contractors are required not to use information about you for any purpose except for those activities we have asked them to perform.

Data Quality and Security

We will take reasonable steps to ensure that your personal information is accurate, compete, up to date and relevant. For this purpose our staff may ask you to confirm that your contact details are correct when you attend a consultation. We request that you let us know if any of the information we hold about you is incorrect or out of date.

Personal information that we hold is protected by:

- securing our premises;
- placing passwords and varying access levels on databases to limit access and protect electronic information from unauthorised interference, access, modification and disclosure; and
- providing locked cabinets and rooms for the storage of physical records.

Corrections

If you believe that the information we have about you is not accurate, complete or up-to-date, we ask that you contact us in writing (see details below).

Access

You are entitled to request access to your medical records. We request that you put your request in writing and we will respond to it within a reasonable time.

There may be a fee for the administrative costs of retrieving and providing you with copies of your medical records.

We may deny access to your medical records in certain circumstances permitted by law, for example, if disclosure may cause a serious threat to your health or safety. We will always tell you why access is denied and the options you have to respond to our decision.

Complaints

If you have a complaint about the privacy of your personal information, we request that you contact us in writing. Upon receipt of a complaint we will consider the details and attempt to resolve it in accordance with our complaints handling procedures.

If you are dissatisfied with our handling of a complaint or the outcome you may make an application to the Australian Information Commissioner or the Privacy Commissioner in your State or Territory.

Overseas Transfer of Data

We will not transfer your personal information to an overseas recipient unless we have your consent or we are required to do so by law.

Contact

Please direct any queries, complaints, requests for access to medical records to:

[insert details of contact person]

Chapter 3: Resources and links

Avant information:

http://www.avant.org.au/News/20131018-mandatory-data-breach/

http://www.avant.org.au/News/20130424-Complying-with-the-new-Privacy-Act-(Cth)/

http://www.avant.org.au/Campaigns/2013/Complying-with-the-new-Privacy-Act-(Cth)/

http://www.avant.org.au/Getting-Started-in-Practice/Risk-Management/Clinical-and-medico-legal-risk-management/Privacy-and-confidentiality/

http://www.avant.org.au/Resources/Public/20130809-privacy-basics/

OAIC information:

The OAIC has released a number of resources to assist you to prepare for the reforms in your organisation:

- Privacy fact sheet 17 — Australian Privacy Principles (APPs)
- Australian Privacy Commissioner, Timothy Pilgrim speaking about the reforms (Youtube)
- Australian Privacy Principles Quick reference tool and summary
- Poster: *Privacy law reform: Get in on the Act*
- Guide to information security: 'reasonable steps' to protect personal information
- APP and NPP comparison guide and APP and IPP Comparison Guide

Strength in numbers gives us strength in defence.
Make Avant your MDO of choice and benefit immediately

Largest specialist medico-legal team	Our in-house legal team has the largest number of specialist medico-legal lawyers of any MDO in Australia.
Best at defending doctors	Our specialist medico-legal team is proud of the landmark cases we have represented and won on behalf of our members – cases that benefit the profession as a whole. Our in-house legal team acts in the best interests of our members. We understand you and your speciality, and this extends beyond just securing the best legal result for you.
24/7 medico-legal support	As an Avant member, receive personalised support through our 24/7 Medico-Legal Advice Service. This service received over 12,000 calls in the past 12 months.
Avant Risk IQ – Risk Intelligence to help you better identify and manage your risk	Avant Risk IQ is a market-leading risk education program that offers a series of resources. Developed using the extensive claims experience and medico-legal risk knowledge Avant has gained from our 60,000 members.
Financially strong mutual	Avant is a mutual, owned by and run for members. As a not-for-profit everything we do is for the benefit of our members, including the reinvestment of any financial surplus.

To find out more call **1800 128 268** or visit **avant.org.au**

Registered Office
Level 28 HSBC Centre 580 George Street Sydney NSW 2000
PO Box 746 Queen Victoria Building Sydney NSW 1230

DX 11583 Sydney Downtown
Phone 02 9260 9000 **Fax** 02 9261 2921

1800 128 268 **avant.org.au**

Avant Insurance Limited ABN 82 003 707 471 AFSL 238765
A subsidiary of Avant Mutual Group Limited ABN 58 123 154 898

February 2014

2612/02-14

Avant
mutual group