Answers to Questions taken on notice from AMA

- AMA Privacy and Health Record Resource Handbook
- AMA Sample Privacy Policy
- Standards for general practices 4.2.1
- Standards for general practices 4.2.2
- Guide to securing personal information "Office of the Australian Information Commissioner"
- HPOS Terms and Conditions of Use and Access.

AMA Privacy and Health Record Resource Handbook

AMA

Privacy and Health Record Resource Handbook

For Medical Practitioners in the Private Sector

Published by AMA, Canberra, 2014

The Privacy and Health Record Resource Kit was written and edited by John Alati, based on the Privacy Resource Handbook, 2010. The law stated herein is applicable as of February 2014.

© Copyright: The Australian Medical Association, Canberra, ACT, Australia. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means – electronic, mechanical photocopying, recording or otherwise, other than by AMA members and their staff for their professional use, unless the permission of the AMA has been given beforehand.

Disclaimer:

The AMA has made every effort to ensure that, at the date of publication, the information contained in this Resource kit is free from errors and omissions and that all opinions, advice and information drawn upon to compile it have been provided by professionals in good faith.

The information and recommendations contained within it are considered to be consistent with the law and applicable Guidelines at the time of publication. However, they do not constitute legal advice. The information provided is not intended to be comprehensive. Medical practitioners concerned about their legal rights and obligations in relation to Federal, State or Territory privacy legislation may wish to seek their own independent legal advice.

Foreword

The AMA supports overarching health privacy legislation and recent updates to improve the privacy of personal and sensitive information in Australia. We believe it is important that the application of general privacy laws to the health sector enhances – not hinders – the provision of quality health care.

We also want to help doctors manage health information in an ethical and lawful way, consistent with the maintenance of high professional standards and quality practice.

Since the first edition of this guide in 2010, The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act) was passed on 29 November 2012. The Privacy Amendment Act introduces significant changes to the Privacy Act, most of which came into effect from 12 March 2014.

The major change that is relevant to medical practices is the new, harmonised, privacy principles that regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs). They replace the Information Privacy Principles (IPPs) that applied to Australian Government agencies and the National Privacy Principles (NPPs) that applied to businesses.

Under the changes, there are 13 new APPs. A number of the APPs are significantly different from the earlierprinciples, including APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information.

The AMA welcomes the enhancements to privacy introduced by the Act, and it is to that end that we provide this guide to assist medical practices to understand and implement their responsibilities in regard to privacy and patient records.

Dr Steve Hambleton

Federal AMA President

March 2014

FOREWORD **3**

A GUIDE TO THE USE OF THIS RESOURCE HANDBOOK **6**

SECTION ONE .....

INTRODUCTION & SUMMARY 8

Federal Privacy Legislation
Related State and Territory legislation ***8***
To whom does the new Federal privacy legislation apply? ***8***

SECTION TWO
The Australian Privacy Principles (APPs) ***9***

Some important notes on information and exceptions ***17***
Permitted General Situations ***17***
Permitted Health Situations ***18***

National Emergencies ***19***

SECTION THREE **20**

PRACTICAL APPLICATIONS OF THE AUSTRALIAN PRIVACY PRINCIPLES 20

Collection ***20***

Do I need my patient's consent to collect their information? ***20***
What do I tell the patient about the information I collect? ***20***
Can I collect information from other sources than the patient? ***20***
Can I collect information from other doctors about a patient without seeing the patient? ***21***
Can I collect information about other family members when taking a medical history? ***21***
Consent ***21***

Is it necessary or advisable to obtain written consent to collect information from patients? ***21***

Use and Disclosure ***21***

Can I release patient information to other doctors? ***21***
Can I share patient information in multi-disciplinary medical teams? ***22***
Special Areas of Concern ***22***

What are the consequences of non-compliance? ***23***
Do Doctors need to have a complaint handling process? **23**
What should Doctors do if the Privacy Commissioner investigates them? **23**
Can I record patient information on a Medical Register? ***23***
Can I disclose patient information to my Medical Defence Organisation? ***24***
Do I have to provide a copy of my whole medical file on that patient? ***24***
Can I discuss patients' needs with practice staff? ***25***
What about where patients don't pay their bills? Can I give patient information to a debt collector? ***25***
Do I have to alter my office layout to comply with the privacy legislation? ***26***
Can I fax and e-mail medical information? ***26***
Can I leave telephone messages? ***26***
How much can I charge to provide access to a patient? ***26***
What are my obligations when I have to disclose information without the patient's consent? ***26***
Do I have to provide access to medical records created before 21 December 2001? ***27***
Can a parent always get access to their children's medical records? ***27***

Can a GP provide a patient access to a specialist's report contained on their file? 27
What if I lose a patient's record? 28
Can I restrict patient access to mental health notes? 28
Do I have to give immediate access to test results? 29
Family History Collection 29
Do I need the consent of family members when taking a family history? 29
Copyright 29
Who owns my medical records – the doctor or patient? 29
Medico Legal Requests 30
Should I forward medical records to a solicitor or a patient's agent? 30
Transfer of Medical Records 31
To whom can I disclose a report prepared for a commissioning agent? 31
I'm retiring – what do I need to do to with my records? 31
A patient wants to change doctors –what am I required to do? 33
SECTION FOUR 34
MEETING COMPLIANCE OBLIGATIONS AND PURSUING BEST PRACTICE 34
Develop and adopt a privacy policy 34
Implementation 34
Privacy audit 34
Disclosure and Complaint Registers 35
Start a Practice Privacy Manual 35
Privacy Action Plan 36
Do you need to appoint a privacy officer? 36
Check the IT Privacy of the Practice 37
Tips on Developing a Privacy Policy 37
SECTION FIVE 39
PRIVACY KIT MATERIAL – TIPS & SAMPLE FORMS 39
Getting Started Checklist 39
Consent Forms 40
Tips on providing access to patients 41
Sample Access Request Form 42
Confidentiality Agreement 44
Sample Privacy Policy 45

A GUIDE TO THE USE OF THIS RESOURCE HANDBOOK

The purpose of this Resource Handbook is to provide assistance to doctors in understanding privacy law and the proper management of health records.

The ***first section*** of the Resource Handbook is a brief introduction to the *Privacy Act 1988* and Australian Privacy Principles (APPs).

The ***second section*** explains and summarises the APPs. Some special areas of concern to medical practitioners are then highlighted and some new concepts are explained.

The ***third section*** deals with the practical application of the APPs to a clinical practice and how doctors can comply with them in the course of carrying out best practice in a busy clinical setting.

The ***fourth section*** provides "getting started" advice on privacy compliance, how to use the AMA's privacy kit material, how to develop a privacy policy to suit the needs of individual practices, and how to move from basic privacy compliance to best privacy practice.

The ***fifth section*** provides the AMA's Privacy Kit and sample forms. The APPs are set out in full in the Appendix to this Handbook.

This Resource kit is not intended to be comprehensive and is not a substitute for a thorough reading of the privacy legislation, the APPs and the guidelines. More importantly, the guide is not a substitute for independent legal advice where necessary. For more information, contact your indemnity insurer or your local AMA.

If there is one overall message to doctors it is the need to ensure open and effective communication between doctor and patient. Effective communication will ensure that the expectations of both doctor and patient are aligned, and that patients have knowledge of their privacy rights, know how their personal information will be managed, and know what they need to agree to if they are to receive prompt and holistic health care. Patients should be made fully aware of any health consequences that might flow if they exercise their right to withhold personal health information from their treating medical team.

Who is this guide aimed at?

This guide is aimed at medical practitioners in the private sector. Those working in public sector institutions should consult their health authority's privacy policies.

The Office of the Australian Information Commissioner has many valuable resources on its website at http://www.oaic.gov.au.

Section One

INTRODUCTION AND SUMMARY

Federal Privacy Legislation

The *Privacy Act 1988 (Cth)* ("the Act"), applies to most of the private sector including all health service providers. From 2014, the Act is subject to amendments introduced by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. The Act incorporates 13 Australian Privacy Principles (APPs) that impose compliance obligations on private and public sector organisations in relation to the management of personal and sensitive information held by them.

Related State and Territory legislation

Section 3 of the *Privacy Act* states that the Act does not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information.

Understanding privacy legislation in Australia is complicated by the fact that there is State and Territory privacy and health records legislation that requires doctors to comply with specific health information management practices. Legislation in NSW, Victoria, and the ACT includes privacy principles that apply to private sector health services. In most respects those principles are similar to the Australian Privacy Principles. They are not dealt with in detail here. Because of the complexities of overlapping laws it is important to seek advice from your local AMA Branch or a legal practitioner if a contentious privacy issue arises.

To whom does the new Federal privacy legislation apply?

The APPs incorporated in the Act are a single set of principles that apply to both agencies and organisations which are collectively defined as 'APP entities'. An entity is defined as:

(a) an agency; or
(b) an organisation; or
(c) a small business operator

Thus, compliance with the APPs is required by all private sector organisations that provide health services and hold health information. This applies to doctors, the people who work within them, doctors practising in partnerships, associateships, or alone, in private hospitals, aged care facilities and other private health facilities, and those who undertake medico-legal work. They also apply to VMOs who work in public hospitals and who retain health records in private clinics.

Section Two

The Privacy Legislation

The *Australian Privacy Principles (APPs)*

The Australian Privacy Principles are the core principles which guide Australian organisations in the management of information. They sit alongside a doctor's significant obligations in the area of confidentiality.

This is not a word-for-word transcription of the APPs. In this section, we have edited the APPs to make them easy to read and understand. This may affect their interpretation in particular situations. If in doubt, it is best to go to the source or seek independent advice.

The Australian Privacy Principles at a glance

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

Australian Privacy Principle 1 - Open and transparent management of personal information

You must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information. It must contain the following information:

- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes for which the entity collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the entity and how to seek the correction of such information;
- how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the entity is likely to disclose personal information to overseas recipients;
- if the entity 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.

You must take such steps as are reasonable in the circumstances to make your APP privacy policy available:

- free of charge; and
- in such form as is appropriate.

If a person or body requests a copy of the APP privacy policy in a particular form, you must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Commentary
This APP is fairly straightforward – your practice must have an up-to-date privacy policy and you must normally make it available free of charge in 'an appropriate form' to those who ask for it. The format is not defined – it may be electronic or in hard copy but, in practical terms, it would be wise to have it available on your website, if you have one, and to have hard copies available for those who ask for it.

Australian Privacy Principle 2—anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with you. This does not apply if:

You are required or authorised by law, or court order, to deal with individuals who have identified themselves; or it is impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym.

Commentary
This means patients have the option of dealing with you anonymously or under a pseudonym unless it is 'impracticable' for you to deal with them in those circumstances, or a law or court order requires you to deal with people who have identified themselves.

This is for a practice to decide, but considering the need to interact with Medicare, keep accurate records, follow up with reports, provide medical reports and ensure reliable payment, it is most likely impracticable for a medical practice to deal with a patient on an anonymous basis. If patients wish to be known generally or addressed by a pseudonym, doctors should respect this as a general right, but it is most likely medical practices will need to deal with people by the name under which they are known to Medicare.

Australian Privacy Principle 3—collection of solicited personal Information

Personal information

This principle applies to the collection of personal information that is solicited by an APP entity, that is, information you ask for.

You must not collect personal information unless the information is reasonably necessary for one or more of your practice's functions or activities.

Sensitive information

You must only collect sensitive information about an individual where:

- the individual consents to the collection of the information, and the information is reasonably necessary for one or more of your functions or activities; or,
- the collection of the information is required or authorised by law or court order; or
- a permitted general situation exists (see below p17) in relation to the collection of the information; or
- a permitted health situation (see below p18) exists in relation to the collection of the information by the entity.

Means of collection

You must collect personal information only by lawful and fair means, and you must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

Commentary

This relates to information that you ask for. That is, 'solicited' information. This means you only collect such personal information (such as name, address) as is necessary to perform your functions in relation to the patient. The same applies to sensitive information (such as health information) unless you are required to do otherwise by law (such as by a court order) or a 'permitted health situation' exists in relation to the situation (see below).

Only collect information by 'lawful and fair' means. This means, in practical terms, by asking the patient directly. You would not, for example, ask for their information from a mutual acquaintance or by some form of secret information-gathering exercise.

Consent becomes an issue here. When a doctor collects information directly from the patient during a consultation, consent is usually implied, so long as it is clear to the patient what information is being recorded and why, how it will be used and to whom it will be disclosed.

The patient is usually the person to give consent but in some circumstances it may be given by a parent or guardian on a patient's behalf. There are occasions where the information collected from the patient is about another person, in which case the consent of that other person might be required.

Australian Privacy Principle 4—dealing with unsolicited personal information

This is about personal information that you did not ask for.

If you receive personal information and you did not solicit the information, you must, within a reasonable period after receiving the information, determine whether or not you would have been permitted to collect the information under Australian Privacy Principle 3 (collection). If so, APPs 5 to 13 will apply to that information, as if you had collected it under APP 3. You may use or disclose the personal information for the purposes of making that determination.

If the information could not have been collected under APP 3, you must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

Commentary

Sometimes patients may send you information you did not ask for, such as medical reports or court orders etc. You first have to determine whether it is the type of information your practice could lawfully have collected. If so, treat it as per APPs 5 - 13.

If you determine that you could not have collected the information, you should first contact the person who sent it to you and arrange to return it. If that is not possible or practicable, you can destroy it. It would be prudent to keep a record of what you destroy and how it came to be in your possession. There is no time frame for this type of action, but be 'reasonable' and be very careful. For example, if a patient sends you an original copy of their mother's will you would determine that this is not the type of information you would be able to collect. It would be prudent to contact the patient and let them know you cannot accept it or store it and arrange for them to collect it, or send it back to them. Keep records of your dealings in these matters to cover yourself.

If it is the type of information you could have collected, such as a patient's medical records (they may have their file transferred to your practice), then deal with the information as you would any other, according to APPs 1-5.

Australian Privacy Principle 5—notification of the collection of personal information

As soon as you collect a person's personal information (such as name, address etc), you must, as far as is reasonable, make them aware of the following;

- your identity and contact details of the practice
- whether you have collected a patient's personal information from someone other than the patient; or if it is not clear that you have collected their personal information, the fact that you have collected the personal information;
- if the collection of the personal information is required or authorised by an Australian law or a court order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);
- the purposes for which you collect the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by you;
- any other body or person or entity to which you would normally disclose the patient's personal information;
- that your privacy policy contains information about how the patient may access and correct their personal information;
- that your privacy policy contains information about how the patient may complain about a breach of the Australian Privacy Principles, and how you will deal with such a complaint;
- whether you are likely to disclose the personal information to overseas recipients; and if you are, the countries in which such recipients are likely to be located if it is practicable to specify those countries.

Commentary

This APP is all about being upfront about how you deal with patients and their information, and how they can correct it if necessary. It emphasises the fact that you have to have a privacy policy containing very specific information.

Be particularly careful here if you have outsourced services such as ICT services to companies which are located overseas. This may mean that your patients' information may be disclosed to overseas recipients.

Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

Where you hold personal information about a patient that was collected for a particular purpose (the ***primary purpose***), you must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

- the patient has consented to the use or disclosure of the information; or
- the patient would reasonably expect you to use or disclose the information for the secondary purpose.

In the case of **sensitive** information, the secondary purpose has to be directly related to the primary purpose. For information that is not sensitive, it needs to be related to the primary purpose.

It is also allowable if the use or disclosure of the information is required or authorised by law or a court order; or a permitted general situation or permitted health situation exists in relation to the use or disclosure (see above), or where you reasonably believe that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Written note of use or disclosure

If you use or disclose personal information in relation to disclosure to a law enforcement body, you must make a written note of the use or disclosure.

Commentary

This APP is about use and disclosure.

Once personal information is collected, the patient's further consent is generally required for its use and disclosure unless the information is being used or disclosed for the main reason it was collected, or for another directly-related purpose, if the person would reasonably expect this.

It is best to err on the side of caution in this regard, not extending 'Primary purpose' to the broad concept of health services or caring for a patient's general health and well-being.

This is also of concern for doctors who need to share patient information with treating teams, some of whom don't see the patient at the time of collection to get consent or discuss purposes of disclosure.

Patient understanding of the purpose of collection is crucial. If the main purpose is for treatment, disclosure, for example, for medical research is a secondary use. Obtaining informed consent to collect information for a holistic approach to patient care – that is, care not restricted to the immediate circumstances, but for the patient's general health - can obviate the need to obtain consents for handling the same information on subsequent occasions. It is therefore important for efficient clinical practice that doctors clearly identify the primary purpose of collecting information and align their expectations with that of the patient.

Australian Privacy Principle 7—direct marketing

If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

An organisation may use or disclose personal information (***NOT*** sensitive information) about an individual for the purpose of direct marketing if:

- The organisation collected the information from the individual; and the individual would reasonably expect the organisation to use or disclose the information for that purpose; and the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and this request has not been exercised; or
- the individual has consented to the use or disclosure of the information for that purpose; or it is impracticable to obtain that consent; and you provide a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and you include in each direct marketing communication a prominent statement that the individual may request not to receive the information.

Commentary

Traditionally, medical practices have not often engaged in direct marketing, but the internet is providing more opportunity for them to do so.

You will need to get consent before sending your own direct marketing material to a patient (unless it is material which the patient would expect to receive from you). If it is not practicable to get consent, then give the individual the chance to opt-out when you do send the material and make sure they know how to contact you to withdraw their consent. Individuals can opt out of direct marketing at any time and you cannot charge

them for doing so. Individuals can also request the source of your information and you must tell them. In most cases in a medical practice, the source will be the patient themselves.

Never use sensitive information for direct marketing unless you have specific permission from the patient to do so. It would be best to get this in writing and, on the whole, probably best to avoid it unless there is a very good reason to do so.

Direct marketing in a medical context is not untenable, but requires great caution. It is strongly recommended that you obtain specific advice before engaging in any direct marketing activities. This does not apply to simple reminders about appointments.

Australian Privacy Principle 8—cross-border disclosure of personal information

Before you disclose personal information about an individual to an overseas recipient you must take reasonable steps to ensure that:

- the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information;
- the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
- there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or the entity expressly informs the individual that if he or she consents to the disclosure of the information, the protections mentioned above will not apply to the disclosure and despite this, the individual consents to the disclosure.

Commentary

This may apply where a patient is moving overseas or going overseas for medical treatment and asks you to transfer their health record to an overseas entity. You have to be reasonably satisfied that there is some privacy protection for that information. If not, you should inform the patient that you cannot be certain their health record will be subject to satisfactory protection and get express permission from them to transfer the record. It would be prudent to do this in writing. If you are in doubt, it may be prudent to advise the patient to seek legal advice on privacy and data protection in the country concerned and get a written statement from them or their advisors to satisfy this Principle.

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

You must not adopt a government-related identifier of an individual as your own identifier of the individual unless the adoption of the government-related identifier is required or authorised by or under an Australian law or a court/tribunal order.

You must not use or disclose a government-related identifier of an individual unless the use or disclosure of the identifier is reasonably necessary to verify the identity of the individual for the purposes of your activities or functions; or

- the use or disclosure of the identifier is reasonably necessary to fulfil your obligations to an agency or a State or Territory authority; or
- the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order.

Commentary
Generally speaking, you must not adopt, use or disclose Commonwealth government identifiers, such as a Medicare or Veterans Affairs number, except for the purposes for which it has specifically been assigned. That is not to say you can't use information such as a patient's Medicare number where necessary. It just means that you shouldn't use it as the means to identify the patient in your practice. You can use or disclose a patient's Medicare number to verify their identity, and in your interactions with organisations such as Medicare.

Australian Privacy Principle 10—quality of personal information

You must take any necessary, reasonable steps to ensure that the personal information that you collect is accurate, up to date and complete, and that the personal information that you use or disclose is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Commentary
This is fairly self-explanatory and straightforward. Practices need to be proactive in updating data. This might include sending regular request to patients to update their details, and updating patient details when they inform you of changes.

Australian Privacy Principle 11—security of personal information

You must take such steps as are reasonable in the circumstances to protect personal information.
If you no longer need the information for any purpose for which it may be used or disclosed and

- it is not contained in a Commonwealth record; and
- you are not required by law, or a court/tribunal order, to retain the information;

you must take such steps as are reasonable in the circumstances to destroy the information or to ensure that it is de-identified.

Commentary
This principle sets standards for protecting and securing health information from loss, misuse and unauthorised access. Again, health service providers must take reasonable steps to achieve this. Paper and electronic records must be properly secured, safely stored and maintained.

This includes safe disposal of data no longer in use. The safe disposal of lap top computers, for example, must take into account the irretrievability of deleted electronic data on it. The safe daily disposal of waste paper bins must take into account identifiable health information on paper scraps. Doctors are probably doing this responsibly, but with the development of e-health their records might need to review and upgrade their security measures.

However, this is not a general licence to destroy records when you no longer need them. Be aware of your obligations in relation to retention of medical records, which are, on the whole, sensitive information but which will almost certainly be linked to a patient's personal information. Be aware that you have obligations under State and Territory laws, and general best practice obligations to retain medical records after a patient has stopped seeing you. This is generally seven (7) years from the last consultation for adults, and up to the age of 25 for children. If in doubt, contact your State or Territory AMA or your medical indemnity insurer.

Australian Privacy Principle 12—access to personal information

If you hold personal information about an individual, you must, on request give the individual access to that information.
Exception to access

A practice is not required to give the individual access to the personal information to the extent that:

- you reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals; or
- the request for access is frivolous or vexatious; or
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- giving access would be unlawful; or
- denying access is required or authorised by or under an Australian law or a court/ tribunal order; or
- if both of the following apply:
    - you have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to your functions or activities has been, is being or may be engaged in; and
    - giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Dealing with requests for access – time and manner

You must respond to the request for access to the personal information within a reasonable period after the request is made; and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Commentary

This APP sets out exceptions to the need to give access to a patient's record. Be very careful when considering denying a patient access to their record. It is probably best to get independent legal advice when you think you should be denying a patient access to their record. This intersects with legislation in NSW, Victoria and the ACT which gives patients a statutory right to access their records.

When a patient asks for access to their record, you must provide it in a 'reasonable' time. There is no definition provided, and it will depend on such factors as how large it is, what form it is in and where it is stored. Also, wherever practicable, give patients access to their record in the form they have asked for. This means, if you have it on a disk and the patient says they don't have access to a computer, you will have to print it for them. It would be best to discuss this need with the patient at the time of the request.

Australian Privacy Principle 13—correction of personal information

If you hold personal information about an individual; and you are satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests you to correct the information; you must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Refusal to correct information

If you refuse to correct the personal information as requested by the individual, you must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by the regulations.

Request to associate a statement
If you refuse to correct the personal information as requested by the individual and the individual requests you to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading, you must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Commentary
You must ensure that the information you have on record is correct. Patients can request it to be corrected. If you refuse, you must set out the reasons why, and allow the patient to 'associate' – or add to their record a statement that the information is incorrect.

Some important notes on information and exceptions

It is important here to note that:

Sensitive information means information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, or criminal record, as well as health information about the person.

Health information includes personal information collected to provide, or in providing, a health service.

Personal information means information or an opinion, including information or an opinion forming part of a database, "whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

This means that consent of the individual is required before any information is collected in the course of providing a health service, unless it comes under one of the strictly defined exceptions.
The amendments to the Privacy Act allow for situations where personal information and health information may be collected, used or disclosed without breaching the Act. These are known as *permitted general situations* and *permitted health situations.*

Permitted general situations
There are seven 'permitted general situations'. An APP entity may collect or disclose personal information where there are:

1. serious threats to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d)).
It is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure and the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

2. Suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d)).
The entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.

3. Missing person (see APPs 3.4(c), 6.2(c) and 8.2(d)).

The entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and the collection, use or disclosure complies with the rules made under subsection (2) above.

4. Legal or equitable claim (see APPs 3.4(c) and 6.2(c)).
The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.

5. Alternative dispute resolution processes (see APPs 3.4(b) and 6.2(c)).
The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

6. Diplomatic or consular functions.

7. Specified armed forces activities – this only applies to the Defence Force.

Permitted Health Situations

There are five 'permitted health situations'. APP 3 and APP 6 contain exceptions where a permitted health situation exists in relation to the collection, use or disclosure of health information or genetic information by an organisation. The permitted health situations in s 16B relate to:

1. Collection - the collection of health information to provide a health service (s 16B(1)) (see APP 3.4(c))
Health information about an individual can be collected where it is necessary to provide a health service to the individual (and the collection is required or authorised by an Australian law other than the Privacy Act); or the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

2. Collection—Research
The use or disclosure of health information for certain research and other purposes (s 16B(3)) (see APP 6.2(d))

3. Use or disclosure—research etc.
Specific provisions exist in relation to use and disclosure of health information in the area of research. If you are involved in research, we recommend you obtain advice in relation to these.

4. Disclosure - or disclosure by an organisation of genetic information about an individual *the use or disclosure of genetic information (s 16B(4)) (see APP 6.2(d))*
Genetic information about an individual can be disclosed where it has been obtained in the course of providing a health service to an individual; and the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and the use or disclosure is conducted in accordance with guidelines approved under section 95AA of the Act (*Guidelines for National Privacy Principles about genetic information*) and the recipient of the information is a genetic relative of the first individual.

5. Disclosure to a responsible person - the disclosure of health information for a secondary purpose to a responsible person for an individual (s 16B(5)) (see APP 6.2(d))
An organisation that provides a health service may disclose an individual's health information where the recipient of the information is a responsible person for the individual; and the individual is physically or legally incapable of giving consent to the disclosure; or physically cannot communicate consent to the disclosure.

It is also permissible where an individual (the ***carer***), providing a health service for the organisation is satisfied that either:

- the disclosure is necessary to provide appropriate care or treatment of the individual; or
- the disclosure is made for compassionate reasons; and the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent; and of which the carer is aware, or of which the carer could reasonably be expected to be aware. The disclosure must be limited to the extent reasonable and necessary to provide appropriate care.

National Emergencies

There are special provisions of the Privacy Act that authorise wide-ranging exceptions to privacy obligations if the Federal Government declares a national emergency. At any time when an emergency declaration is in force an entity may collect, use or disclose personal information relating to an individual if you reasonably believes that the individual may be involved in the emergency and the collection, use or disclosure is in relation to the emergency. In these cases, you may disclose relevant personal information to an agency or an entity that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency; or a person or entity prescribed by the regulations, by the Minister, or by legislative instrument. This does not authorise disclosure of personal information to the media.

Privacy Tip

The Privacy Act distinguishes between 'personal information' and 'sensitive information'.
Personal information includes:

- name or address of a person
- bank account details and credit card information
- photos
- information about your opinions and what you like.

'Sensitive information' includes health information and genetic information about an individual that is not otherwise health information. It also includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices; or
- criminal record.

At times they are treated differently under the Act. Medical practices will normally collect both types of information.

SECTION THREE

PRACTICAL APPLICATION OF THE AUSTRALIAN PRIVACY PRINCIPLES

Tracking Information

Document what personal information is collected and how it is used. It is recommended that you put in place systems which enable you to track data from its point of collection through to use, storage, de-identification and destruction.

Hardware

Mobile devices, laptops, hardware and USB devices all need to be stripped of data when they are disposed of or retired from service.

Collection

Do I need my patient's consent to collect their information?

Yes, but this is generally implied by the patient presenting for medical attention and giving the doctor the relevant medical history for that purpose.

There are exceptions to the requirement for consent, such as where it is necessary to deal with a threat to the life or health of an individual who is physically or legally incapable of giving the consent. The exceptions are set out in APP 3.

What do I tell the patient about the information I collect?

Most patients will agree as a matter of course to providing personal information to the practice and sensitive information to the doctor. See APP 1 for information on collection of data. Bear in mind your primary purpose is usually going to be provision of health care. If that is not the case, you will need to make things clear.

Unless the doctor's and patient's expectations about the main purpose for which the information is required are aligned, a myriad of consents might be required for later use and disclosure of the information in the course of the patient's health care. See **Use and Disclosure p21.**

The patient has to be advised how their information will be handled. The patient should be informed that information will be collected, the purpose of collection, that they may access information collected about them, and to whom the information will be disclosed. General information about this can be set out in a patient information pamphlet.

If possible, the patient should be told how their information will be handled at the time of collecting the health information. Often, when the patient first sees their doctor, the advice can be given during usual communications. The patient might be handed an information sheet or pamphlet and also be given information orally during the consultation.

Can I collect information from other sources than the patient?

Collection should primarily be from the patient, but may come from other sources, for example, x-rays and specialists' reports. Sometimes information about a patient is volunteered from family or other sources. Unless it would be a serious threat to the life or health of any individual, the patient should be informed that information has been collected, the purpose of collection, that they may access the information and to whom the information will be disclosed.

Prescription Shopping Information Service (PSIS)
Under the PSIS program, the Department of Human Services can disclose certain information about PBS medicine obtained by patients without the patient's consent for limited purposes.

Can I collect information from other doctors about a patient without seeing the patient?
Radiologists, pathologists and, in some circumstances, anaesthetists often collect patient information without seeing the patient, or in circumstances not conducive to informing the patient about the collection, use and disclosure likely to occur in relation to their personal information.

If the referring doctor has sufficiently explained the purpose of collecting a medical history at the time of taking it, and the patient understands that the information would be used for this type of ongoing health care, members of the treating team could reasonably proceed without the need for further specific consents.

Radiologists, pathologists and other specialists might also comply with the Act by informing the patient of the way in which their information was handled, say, by including an appropriately drafted statement on the back of the patient's account. An example of such a statement is available in Section Five.

Can I collect information about other family members when taking a medical history?
While consent for this is required under the privacy legislation, the Federal Privacy Commissioner has issued a Public Interest Determination (PID 12 in force until 10 December 2016) that exempts compliance with this requirement. For details of the exemption see **Family History Collection**.

Consent

Is it necessary or advisable to obtain written consent to collect information from patients?
The Act is not prescriptive. The doctor has to be satisfied that a person genuinely consents to the collection of their personal information.

Consent can be express, oral or implied. It is implied, for example, where a patient gives a medical history to the doctor when presenting for treatment. What is important is that the consent be voluntary and informed.

The fact that a patient presents for health care and freely gives their information will generally be evidence of consent. Contemporaneous notes usually provide the best evidence of what has occurred.

Where the doctor has any doubts, express consent should be obtained and noted. Consent forms are not obligatory, but may be necessary in some situations. Obtaining written consent is advisable, for example, where the use of patient information is requested for secondary purposes, such as scientific or market research. A sample consent form is provided in Section Five.

Use and Disclosure

Can I release patient information to other doctors?
Once the doctor has collected patient information it may be used or disclosed for the main reason it was collected or for another directly related purpose if the person would reasonably expect this. Otherwise, further consent is required for its use or disclosure.

If the main purpose of collecting patient information is for clinical care, then the use or disclosure of that information to others in the treating team for that particular episode of care, is a directly related secondary disclosure that is likely to be within the reasonable expectation of the patient, and further consent is not required. On the other hand, its disclosure for the purposes of medical research is an unrelated secondary use that requires patient consent.

It is therefore important that doctors obtain their patient's agreement to collect information from them for the broader purpose of caring for their health as a whole, if that accords with their general practice, and ensure that they have aligned their expectations in that regard with those of the patient. Further consent is not then required for the consequent sharing of information with other doctors in the course of caring for the patient's health needs.

Can I share patient information in multi-disciplinary medical teams?
The multi-factorial nature of some medical conditions, such as psychiatric disorders, usually requires multi-disciplinary involvement with management and hence, communication between various organisations for whom the involved health professionals work. The need for consent at each and every instance of 'extra-organisational therapy' is impractical and can be avoided if, at the outset, the patient understands and consents to the sharing of information between the treating team for the holistic care of the patient.

For further information, see the AMA's position statement: *Guidelines for Doctors on Disclosing Medical Records to Third Parties 2010;*
Available at: https://ama.com.au/position-statement/guidelines-doctors-disclosing-medical-records-third-parties-2010

Personally Controlled Electronic Health Records Act 2012

The *Personally Controlled Electronic Health Records Act 2012* (PCEHR Act) provides controls on the collection, use and disclosure of information in an individual's eHealth record. Any collection, use or disclosure not authorised by the legislation is a breach of the PCEHR Act and the Privacy Act. The OAIC regulates the handling of personal information under the eHealth record system by individuals, Australian Government agencies, private sector organisations and some state and territory agencies.

Special Areas of Concern

Access to Medical Records
Patients have a general right to access all health information held about them. Some exceptions exist, such as where:

- it would pose a serious threat to anyone's life or health;
- it would have an unreasonable impact on someone else's privacy;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the organisation and the individual and the information is the subject of professional legal privilege;
- it would be unlawful to provide access, or denial is authorised by law; and
- it might prejudice an investigation of possible unlawful activity.

Handling requests for access
Organisations need to develop a policy to outline how they will handle access requests. Patients do not have to give reasons for requesting access. However, the scope of the request may need to be clarified in order to provide appropriate access, which may not necessarily involve providing a copy of the whole of the patient file. The patient might only want to look at the notes during a consultation, or may want copies of documents on their file. Generally, a patient should be allowed access in the form requested. Patients cannot be required to make their requests in writing, though in some cases it may be prudent to request the patient to do so.

A patient's request for access should be noted on the patient's file, and all requests should be referred to the treating doctor. The request should be completed within a reasonable time, taking into account the patient's needs, and should not ordinarily exceed 30 days.

Fees that can be charged

Patients should be made aware of the costs charged where a doctor's time or administrative overheads are involved, and be given the option of less costly forms of access. (See Section Three under *Access*).

Location of Patient Information

The Act does not concern itself with who owns the health records, but applies to individuals and organisations that hold personal and health information. In other words, who controls the records is the determining factor as to whether the records fall under the Act or not. It is possible for medical records, as they move around, to be covered by the Act at some times, and not at others. It is also possible that the same set of notes can be shared by a number of people, some of whom are subject to the Act and some who are not. To assist in understanding this movement of records, consider the following situations:

- a doctor who works for a State/Territory health organisation and bills public patients – the medical records held by the public entity, and are exempt from the Act, but may be subject to relevant State/Territory privacy or health records legislation;
- a doctor who works at a State/Territory health organisation and with a right to see private patients – the medical records are held by the doctor and subject to Act;
- a doctor who works at a State/Territory health organisation and bills public patients, but takes copies of patient information back to their private rooms – the medical records held by the public entity are exempt from the Act but are subject to any relevant State/Territory health records or privacy legislation. However, once the doctor takes possession of a copy of the records, then those records are subject to the Act; and
- a doctor who works in private rooms and bills patients privately – the medical records are covered by the Act.

If there is any doubt as to the control of any patient records, a doctor in private practice should comply with the Act.

What are the consequences of non-compliance?

The Office of the Australian Information Commissioner has greater powers to investigate and the ability to impose penalties of up to $1.7million for those found to be in breach.

Medical Indemnity cover for privacy breaches

Doctors are advised to check whether their professional medical indemnity arrangements cover awards and/or the costs of investigations and representation.

Do doctors need to have a complaint handling process?

Yes. In the majority of cases, the matter should be able to be resolved to the patient's satisfaction by simply discussing the issues with the patient. Only on failure of that process will the Commissioner look into a complaint. An investigation could be time consuming and costly to the practice.

What should doctors do if the Privacy Commissioner investigates them?

Doctors are advised to obtain their own independent legal advice and/or notify their MDO. In addition, AMA members are invited to notify the Federal AMA office of any investigation by the Commissioner. Doctors and their staff should comply with any direction given by the Commissioner, as monetary fines or imprisonment may result from non-compliance.

Can I record patient information on a Medical Register?

If a doctor suggests a diabetes test and the patient agrees, then consent to collect relevant information about this condition is implied. The use to be made of the information and to whom the information is likely to be disclosed and why, should be explained at the time of collection. The information, once collected, can be used

(within the practice) and disclosed (outside the practice), such as to other members of the treating team, in the event that treatment for the condition is required.

However, there is an issue when patient health information is recorded on medical registers, such as a diabetic's register. Although recall/reminder systems are directly related to the patient's health, if registers are used for this purpose, as the information is being recorded somewhere other than on the patient's file, and particularly if the register system is to be used to facilitate government practice incentive payments, the purpose of the register should be explained to the patient. A patient's agreement is required if the register is held outside the practice, such as registers held by GP Divisions or Medicare Locals. The doctor should ensure that the patient agrees to the method of recall/reminder. That is, whether it is in order for a phone call to be made and a message left with the person who answers the phone, or a recorded message, or whether the reminder should be by way of letter only. Otherwise, an unlawful disclosure might inadvertently be made.

Do I have to provide a copy of my whole medical file on that patient?

What the patient requires should be clarified, and the appropriate format in which it should be provided should be discussed. A patient may not want the whole of the record. They may be happy to receive a summary of the notes or of a specialist's opinion, or receive an explanation, or simply want a copy of a test report. Generally access should be provided in the form requested. That may mean providing a copy of the document or documents containing the information, rather than just an opportunity to view the file or to attend for a consultation about the information. It is not sufficient to provide illegible notes or incomprehensible computer print outs. The cost of any elaboration or rewriting should also be made clear prior to providing the documents to the patient.

Case note:
B v Surgeon [2007] PrivCmrA 2
The complainant had been the patient of a surgeon and had sought a copy of their medical records.
The surgeon advised the complainant that they could view their medical record under the supervision of a staff member but they would not provide a copy of the medical record. The patient wrote again seeking a copy of the medical record, or in the alternative, an explanation as to why the surgeon could not give the complainant a copy of the medical record.
The surgeon provided partial access to the record. This did not include copies of consent forms, quote sheets and registration pages. The surgeon said that the reason these documents were excluded was because the surgeon considered them commercially sensitive as they were generated with templates specifically designed by the surgeon and the surgeon did not want these documents made available to commercial competitors.
The Commissioner did not form a view on whether the Privacy Act required the surgeon to provide access to the material that was withheld. On confirmation that the complainant had received copies of the relevant documents the Commissioner was satisfied that the respondent had sufficiently addressed the complaint and closed the complaint under section 41(2)(a) of the Privacy Act on the grounds that the respondent had adequately dealt with the complaint.
This case is not conclusive, but seems to indicate that 'reasonable access' does not have to include documents that are not relevant to the patient's clinical care. Caution should be exercised.

Can I disclose patient information to my Medical Defence Organisation?

Patients are more likely to reasonably expect this if it is set out in an information sheet supplied to them. However, the Privacy Commissioner has acknowledged that doctors may be obliged to disclose patient information relating to adverse outcomes to their Medical Defence Organisation, insurer, medical experts or

lawyers without the patient's consent. Professionals such as lawyers are bound by strict privacy and confidentiality protocols. Disclosure may be compelled by court order. In any event, a patient cannot reasonably expect to launch an action if they are not prepared to disclose relevant information.

Can I discuss patients' needs with practice staff?

Case note:

F v Medical Specialist [2009] PrivCmrA 8
The patient had been treated by several health professionals at the same clinic, and asked to be treated by a specific consultant.

The consultant refused the complainant's request for treatment and subsequently discussed the complainant with the clinic manager. The complainant claimed that the consultant had unnecessarily disclosed their personal information to the clinic manager.

The consultant then advised the clinic manager of the complainant's need for treatment, the consultant's personal refusal to treat the complainant and the reasons for this refusal.
The Commissioner formed the view that in the circumstances described, the disclosure of the complainant's personal information to the clinic manager was both directly related to the purpose for which the information was collected, and was within the complainant's reasonable expectations.

What about where patients don't pay their bills? Can I give patient information to a debt collector?

Case note:

L v Health Service Provider [2009] PrivCmrA 15
The complainant underwent a medical procedure and received an invoice from the health service provider, which remained unpaid. The health service provider sent several follow up invoices and a final letter of demand advising that it would list a payment default on the complainant's credit file if the invoice was not paid. The health service provider subsequently listed the payment default. While the complainant had failed to pay for the medical procedure, the Commissioner considered the health service provider did not have a sufficient credit relationship with the complainant, and was not a credit provider. The Commissioner formed the view that the health service provider had interfered with the complainant's privacy by listing a payment default when it was not a credit provider in respect of the debt.

Names and addresses recorded by doctors must be afforded the highest level of privacy. Generally, such information should only be used for the primary purpose of collection, or for a directly related secondary purpose which is in the patient's reasonable expectation. Using the patient's name and address details for billing purposes, and for the purpose of chasing up non-payment, may arguably fall into the category of directly related secondary purposes within the patient's reasonable expectation. Patients would reasonably expect doctors to chase unpaid accounts. However, in light of this decision, care needs to be taken. It seems it is not generally permissible to disclose a patient's name and address to a debt collection agency to recover a bad debt, although it may arguably be a permitted general situation involving pursuing a legal or equitable claim.

Practices may consider a carefully worded consent for this when they take on a new patient.

Do I have to alter my office layout to comply with the privacy legislation?
Accidental disclosure of patient information can occur if discussions between the receptionist and patient can be overheard.

Doctors should ensure the reception desk is designed to protect patient information, and to make staff aware of the need to position themselves in such a way that telephone conversations are not likely to be overheard, and that unnecessary identification of patients is not made. Similarly, doctors calling in their patients by name should exercise discretion. Patients might also be given the option of completing a form rather than answering questions asked by the receptionist.

Can I fax and e-mail medical information?
There is nothing specific to prohibit electronically transmitting health information, as long as you take reasonable steps to ensure that the information is secure in transmission.

Can I leave telephone messages?
Unwitting breaches of patient privacy can occur by a medical practice leaving a message with a person or on an answering machine when a patient is not available. Medical practices should not leave telephone messages that include sensitive information, unless that is authorised by the patient on a case-by-case basis.

What are my obligations when I have to disclose information without the patient's consent?
If disclosure is permitted or required by law, such as the notification of a communicable disease, the patient should, where practical, be informed of that having occurred. Doctors are required to keep a register of disclosures made to an authorised enforcement body (see APP 6).

How much can I charge to provide access to a patient?
Patients cannot be charged application fees to lodge a request for access, or for legal advice obtained by the doctor relating to a request for access. They can be charged a reasonable fee to cover administrative costs, the costs of photocopying, retrieving information, etc.

What the doctor and patient may consider to be a reasonable cost for complying with the request for access may differ. Guidance can be sought from other relevant legislation that provides for photocopy costs, such as might be contained in Freedom of Information or Health Records legislation.

NB: In Victoria only, refer to the *Health Records Regulations 2012* for a schedule of fees.

Case note: D v Health Service Provider; E v Health Service Provider; F v Health Service Provider; G v Health Service Provider [2005] PrivCmrA 4

When assessing whether charges imposed by an organisation for the granting of access are excessive, the Commissioner considers each complaint independently because access charges can vary widely. The Commissioner generally considers the following factors:

- the number of pages in the record;
- the method of storage (electronic, paper based, audio, visual);
- the retrieval process involved (whether the file is stored off site, or archived);
- the cost incurred by the organisation for providing access, including staff time and photocopying costs;
- whether charges enforced are commensurate with the task performed (for example a specialist cannot carry out the task of photocopying documents and charge for this service at the specialist's hourly rate);
- the individual's capacity to pay for access (pensioner, student); and
- the form in which an individual requests access to documents.

The Commissioner also considers that costs incurred in obtaining legal advice regarding obligations under the Act should not be passed on to the applicant.
The Commissioner was of the view that flat fees for granting access will be considered to be excessive in cases where the particular costs associated with providing access to an individual do not justify the flat fee.

Do I have to provide access to medical records created before 21 December 2001?

The Act generally applies to information collected on or after 21 December 2001. However, personal information collected before that date that is still in use forms part of the post-21 December 2001 record, to which the patient has access. Past records are 'still in use' if they relate to a condition still being treated, or they are referred to in the course of continuing health care. If providing access to past records causes an undue financial or administrative burden, then a summary of the relevant part of the records will suffice. There is, therefore, no obligation on a doctor to provide access to a patient of past records not in use. However, a request for access to these records should be handled in accordance with good clinical and ethical practice.

Can a parent always get access to their children's medical records?

The Act does not specify an age at which a child is considered of sufficient maturity to make his or her own privacy decisions. Doctors need to address each case individually, having regard to the child's maturity, degree of autonomy, understanding of the relevant circumstances, and the type and sensitivity of the information sought to be accessed.

In the case of a baby the circumstances are likely to be rare where there are real concerns for the child's health that can't be disclosed to the accompanying parent, or which did not warrant outside intervention.

In the case of a young teen, the doctor might quite properly take the view that access to the records without the child's consent would be a breach of confidentiality. The request for access should then be treated as a parental request for disclosure, and denying the parent access requires no reason other than confidentiality having to be maintained.

However, if a doctor suspects that **parents are using the child's health for their own domestic purposes**, as might occur in a family law context, the doctor will need to ask which parent is entitled to receive information about the child. If the matter can't easily or quickly be resolved and the child has health needs that require attention, it would be prudent to advise the absent parent of the disclosure made to the accompanying parent.

Can a GP provide a patient access to a specialist's report contained on their file?

Patient access to a GP's medical records includes access to specialists' reports on the GP's files, notwithstanding that they may be marked "not to be released to the patient". A notation "not to be released

to a third party without my permission" is also to be ignored if the patient authorises the release, or the law requires it. However, specialist notation of this kind may alert the referring doctor to something in the report that might cause serious harm to the patient or another person, and thus provide a reason for restricted release. Otherwise, the specialist's consent to patient access is not required. Generally, specialist reports form part of the patient's health record and should be treated as such.

What if I lose a patient's record?

Case note: V v Health Service Provider [2006] PrivCmrA 21

A complaint was made concerning the health service provider's loss of the complainant's medical record, dating from their birth. The health service provider had conducted a search of its current and archived records, but was unable to locate the complainant's record. The health service provider advised the complainant that it was likely that the complainant's medical record had been misfiled. The health service provider apologised, and advised that it had attempted to reconstruct the medical record using information that was available electronically, or available from other originating sources.

The health service provider advised that it maintained around 100 000 medical records and supplied the Commissioner with details of its record management system for patient records. The health service provider confirmed that it had undertaken a comprehensive search for the complainant's medical record, both on and off-site, but had failed to locate it. It stated that it could not fully account for the circumstances surrounding the loss of the medical record, however it believed it had been misfiled as a result of human error.

The Commissioner was of the view that the health service provider's record management policy, which included access controls, physical security measures and storage, archiving and shredding protocol, was reasonable, and that it appeared that the misplacement of the medical record was the result of human error and not the result of a systemic procedural problem on the part of the health service provider.

The Commissioner also noted that in this instance, where the health service provider's record management practices had failed, the health service provider had made a significant effort to locate the records and then to reconstruct the medical record as comprehensively as possible. The Commissioner formed the view that, in taking these steps, the health service provider had adequately dealt with the complaint.

Can I restrict patient access to mental health notes?

GPs and specialists such as psychiatrists collect information and make process notes of a highly intimate and often controversial nature.

Where access to the notes is requested, doctors should consider issues such as whether providing access would pose a serious threat to the patient or to any other person, or whether providing access would have an unreasonable impact upon the privacy of another, including the doctor.

Means of providing access other than by copying complete notes may be considered, including the provision of a summary report. However, generally access should be provided in the form requested. A psychiatrist or psychotherapist might find it helpful to let patients know in advance that most of the material collected from the patient will be in the form of psychotherapy 'process notes', rather than factual material, and that it is often the case that patient access to such notes is restricted on the grounds that access and correction of the notes might impede the therapeutic process and cause serious harm to the patient. It could be explained that a summary only of this material is usually provided in response to a patient request for access. Upfront, open communication with patients is to be encouraged. However, no agreement should be reached to this effect as

a matter of course as, in the event that a patient does insist on a full copy of the notes after being offered a summary, then the situation has to be revisited to see if a restriction is warranted under the Act.

Do I have to give immediate access to test results?
If a patient pre-empts a medical appointment and requests access to test results before discussing the report with the doctor, the access should be deferred until the consultation has taken place. By way of contrast, if a patient asks for a copy of a report dating back 12 months, after appropriate clinical interventions have occurred, the practice's procedures for access requests (which may still include reference to the doctor) should be followed.

Family History Collection

Do I need the consent of family members when taking a family history?
Best clinical practice often requires collecting a full family and social history from patients.

The Privacy Commissioner has addressed this by issuing a Public Interest Determination (PID 12) (which is in force until 10 December 2016), which declares that no organisation is taken to contravene the Act if health information is collected by a health service provider from a patient about another person ('the third party') in circumstances where:

- the collection of the third party's information into the health consumer's family, social or medical history is necessary for the applicant to provide a health service directly to the health consumer; and
- the third party's information is relevant to the health consumer's family, social or medical history; and
- the applicant collects the third party's information without obtaining the consent of the third party; and
- the third party's information is only collected from a person responsible for the health consumer if the health consumer is physically or legally incapable of providing the information themselves.

The Determination provides that, in that situation, the public interest outweighs the interest in upholding the third party's privacy.

Copyright

Who owns my medical records – the doctor or patient?
As a general rule, the doctor who holds patient information owns and controls it. Doctors retain their legal rights in relation to copyright of their own work. The Act gives patients a general right of access to information held about them.

Included in the health information a doctor often holds about a patient are diagnostic notes, perhaps a medical protocol tailored to a patient's particular needs, letters written by the doctor, and clinical notes taken about the patient, to which the doctor owns the intellectual property rights. The copyright of specialists' reports held on a GP's file belongs to the specialist who wrote the report. The way in which the doctor takes notes, records patient management and so forth form part of the doctor's intellectual property.
However, a patient's right to access their health information may be subject to restrictions as to its reproduction and use, subject to the doctor's permission. Where necessary, this may include ensuring that the doctor's opinion is not reproduced by someone for commercial purposes without the doctor's permission, and there is the question of the right to charge a fee for reports.
There is nothing to stop a doctor from asserting copyright over the material that indicates that the doctors' consent is required for further reproduction of the material. However, the doctor should ensure that this does not breach his/her ethical duty by preventing relevant material being made available to another doctor or medical treatment team member.

Medico Legal Requests

Note: Great care should be taken when considering access to medical reports and records in a medico-legal context. Legal procedures such as disclosure, production and privilege can be complex when interacting with privacy legislation. If you are unsure it is advisable to contact your indemnity insurer, local AMA, or to seek independent legal advice. It is always best to clarify with the party commissioning the report, such as an insurer, what the legal status of the report will be once it is completed. Some examples are provided below as a guide only, and should not be relied upon as setting out a definitive legal position.

The Act provides patients with a general right to access personal information held about them. Opinions expressed in medical reports prepared at the request of lawyers on behalf of clients form part of the health record to which the Act applies. The intellectual property rests with the author of the report. But, subject to certain exemptions, a person is entitled to know and see what information is held about them. Sometimes a person requests a copy of a medico-legal report written about them but commissioned by another party. Consider these situations:

1. where a doctor, who is not the treating doctor of a patient, is requested by a third party - such as an insurer of a defendant to a legal proceeding – to prepare a medico-legal report. The patient's consent is required before the patient is examined by the doctor for the purpose of preparing the report. The report, commissioned by a third party, may be subject to legal professional privilege, and exempt from the access requirements under the Act, but this should not be assumed. You should check the status of the report with the insurer;

2. where a third party commissions the report – say for insurance purposes rather than for legal proceedings – no legal professional privilege applies. The patient is, subject to other restricted exemptions under the Act, entitled to access that report. Doctors might be concerned that a patient might then use the report for other purposes – for pending litigation, or for some other commercial purpose such as to obtain a pilot's licence. While under the Act the doctor is not entitled to ask a patient why access is required, in the case of a medico-legal report, it is reasonable for the doctor to assert copyright over it. In that event, the doctor can provide access on the condition that the report not be further published or reproduced without the doctor's permission. In this way the doctor can then ascertain whether the patient was attempting to use the Act to avoid paying the appropriate fee; or

3. where the treating doctor has been asked to provide a report for medico-legal or other commercial reasons, on behalf of the patient. Though a commercial fee for the preparation of the report is agreed, the patient accessing the report through the Act could circumvent its payment. Where a doctor has concerns about this occurring, the problem might be avoided by the doctor asking for the agreed fee to be paid before the patient is examined and the report prepared.

Should I forward medical records to a solicitor or a patient's agent?

Where a patient asks for their notes be forwarded to their solicitor, or a solicitor representing a patient asks for their health record, it is likely that the material is to be used for medico-legal purposes. It is improper for lawyers to use the Act as a back-door method of obtaining access to medical opinions. A simple request from a solicitor is not a court order. If litigation is on foot and discovery procedures are in place, this should be clarified with the solicitor concerned.

It would be appropriate to ask the patient or solicitor to clarify what part of the notes is required. The doctor then, as in every case where copies of the whole or part of a file are required, should go through the notes to

identify any information to which access should be restricted (such as information about other people collected in the course of history taking). Then, whether part or all of the notes are required, the doctor should request that the reasonable administrative costs incurred in the doctor reviewing the notes and the photocopying costs be paid before their release to the solicitor.

To whom can I disclose a report prepared for a commissioning agent?
If you are not the treating doctor, and you are commissioned by a third party to prepare a report on a patient, if the report is for the purpose of litigation, it may be the subject of legal professional privilege. The patient has no right of access to it, though it can be disclosed to the commissioning party. The patient has consented to an examination and the report being prepared, and would reasonably expect it to be used and disclosed for the purpose for which it was prepared.

If the report was commissioned for other purposes, say for production to a Mental Health Tribunal or Parole Board, the disclosure is authorised or permitted by law, whether or not the patient has consented to the disclosure. Generally speaking, the patient is likely to be able to access the report, but you should check with the entity commissioning the report.

In some states Work Cover legislation authorises the release of information to a statutory board, and requests are made to doctors for information without providing the patient's consent. Generally, the patient having made application for some benefit under the Work Cover legislation covers the consent requirement. If the release of information is authorised by the relevant legislation, no further consent is required. But good clinical practice would surely dictate that the doctor should inform the patient of the request, and of the fact that it has been met.

If an insurance company or employer commissions the report, so long as the person has given authority for the report to be prepared, then it follows that the report can be disclosed to the commissioning agent, the purpose for which the material was collected. However, if an employer seeks information from a doctor to verify a sickness certificate, the doctor should obtain the patient's consent before dealing with this inquiry. Similarly, if a family member makes an inquiry as to whether or not a patient has made an appointment to see the doctor, this information should not be given without the patient's consent, if the patient has capacity or maturity to make their own decisions about the management of their health information.

These situations can be complex and subject to legal procedures and professional privilege. If in doubt, it is entirely appropriate for a doctor preparing a report to clarify with the entity commissioning the report what its status will be, and mark it appropriately for the benefit of staff. ***Always seek legal or expert advice if you are unsure.***

Transfer of Medical Records

I'm retiring – what do I need to do to with my records?
Where a practitioner retires and another doctor within the practice takes over responsibility for the patient records of the retiring practitioner, it is appropriate for a circular to be sent out notifying of the retirement and to include notice that the records will be held by the nominated doctor in the practice. If that is not feasible, then it is appropriate to inform each patient, as they contact the practice, of the new arrangement, so as to allow a patient the opportunity of having the records transferred to another doctor or practice.

If no arrangements can be made to transfer the records to another doctor, then suitable storage arrangements should be made so that they can be easily accessed if required, and the practices' phone number might have to be retained or redirected to ensure patients can be informed of the new arrangements.

Case note:

H v Health Service Provider [2010] PrivCmrA 9

Facts:
The complainant was a patient at a health clinic that was sold to another health service provider. The complainant alleged that the purchasing health service provider did not have their authority to collect their sensitive information and also failed to provide them with notice of collection at the time it acquired the health clinic.

The Commissioner found that the original health clinic had placed a notice on behalf of the purchaser at the clinic outlining details of the sale of the business, the identity of the purchaser, how it could be contacted and notified individuals that they were able to gain access to their health information. The complainant was also personally informed about these issues prior to the sale. Therefore, the Commissioner formed the view that the health service provider had met the notice requirements of the Act.

The Commissioner considered whether the collection was necessary to provide a health service, given the complainant may not have attended the new service. The Commissioner took the view that the collection was necessary for the continuation of the health service to the individual. If the collection did not occur the health information would be lost as no organisation would be responsible for it.

Third, the purchasing organisation advised that it was a member of a competent medical body whose code of practice requires its members to maintain the confidentiality of client information and to comply with current privacy legislation. Therefore, the Commissioner was satisfied that the collection was in accordance with rules established by a competent medical body.

The message from this decision is clear – you must let patients know if you are closing or selling your practice.

***Tip: Have a succession plan in place well before it's needed*!**

No doctor wants to think about the possibility of having to cease practice suddenly. There are a range of factors that can cause a practice to close quite suddenly. These include illness, death and insolvency. But doctors are human beings too, and it does occasionally happen that a doctor has to cease practice without much, or any, warning.

For this reason you would be well advised to have a succession plan in place to cover these situations, just like you have insurance in place but hope you'll never need it.

If you don't, then others are usually left with the difficult task of having to deal with years of accumulated records and requests for access.

It is not possible to say definitively what to do in this situation, but generally you need to make some provision to inform patients when a practice is about to close, and give them the choice of collecting their records or having them transferred to another practice. Make provision for archiving records that are left for as long as possible. Here you would generally follow the State/Territory guidelines for retaining health records, seven years for adults and up to the age of 25 years for children. If you have files which are likely to be contentious or give rise to litigation, be prepared to retain them for as long possible. You should contact your indemnity insurer for further advice.

A patient wants to change doctors –what am I required to do?

A doctor should always do what accords with best clinical practice and relevant codes of ethics, to ensure that all papers and records the new practitioner would reasonably require to adequately treat the patient are provided.

If the patient has requested the full medical file to be transferred, then the patient's wish should be met, with copies of the file being provided to the nominated doctor. The transferring doctor should retain all original documents on his/her own file and archive for medico-legal purposes.

The author of material on the doctor's file is irrelevant, as the practitioner who holds the material is responsible for complying with the request for access/transfer.

It may be appropriate to clarify the scope of the patient's request, to understand the needs of the patient and the new treating practitioner. You may charge a reasonable fee for this service.

Section Four

MEETING COMPLIANCE OBLIGATIONS AND PURSUING BEST PRACTICE

Develop and adopt a privacy policy

1. The first obligation under the Act is to develop a privacy policy in compliance with the Act. For 'getting started' purposes, a medical practice might initially adopt the policy as set out in the sample in this guide. Conduct a privacy audit of the practice to see where deficiencies in compliance with the Act by the practice lie.
2. Adjust the adopted privacy policy as required to ensure the policy reflects the particular procedures of the practice.
3. Nominate a person in the practice as privacy officer who is responsible for:
    - full implementation of the policy;
    - the handling of staff and patient privacy questions;
    - setting up access request and complaint handling mechanisms; and
    - ongoing privacy compliance.

Implementation

Much of the compliance obligation is to ensure that a patient is aware of the practice's privacy policy and procedures for handling personal information. This can be achieved by carefully worded waiting room notices or posters, patient information sheets, and a practice privacy policy pamphlet. Nothing, however, will be a substitute for frank and effective doctor-patient communication.

Privacy Audit

Take a look at the reception area:

- Can the risk of telephone conversations being overheard be minimised?
- What can be done to minimise the risk of patients being overheard when giving oral information?
- Are computer screens and patient records out of view of other people?
- Are screen-savers fitted to block unauthorised viewing?
- Is access to patient data restricted to those who require it?

Take a look at your consulting habits:

- Do you keep patient information – files, medical reports, mail or scripts bearing patient names – out of the view of other patients?
- Do you remove data displayed on a computer screen relating to a previous patient before the next patient comes in?
- Do you take care when taking telephone calls relating to a patient in the presence of another patient, not to identify the patient when health information is discussed?
- Do you ensure that staff, registrars, students, non-treating doctors or nurses-in-training are not present during consultations without the prior permission of the patient?

Take a look at your existing forms for patient completion:

- Do they ask only for information necessary to be collected for the provision of the health service and associated administrative purposes?
- Do they state that the patient is not obliged to provide any information, and set out the consequences, if any, that may result if the information is not provided (e.g, that the service cannot be provided)?
- Do they require written consent regarding the collection of information and, if so, is sufficient information provided to ensure that the patient's consent is fully informed? Are procedures in place to ensure that the consent is genuinely given?

Take a look at patient records. Are there procedures in place :

- for noting – say in red ink – on patient records any restrictions on access, use or disclosure?
- For noting when anyone else accesses sensitive information?
- For distinguishing between information collected before 21 December 2001, and that collected after that date, to reflect the different obligations that apply to access, use and disclosure?
- To review personal information regularly, and to securely destroy records no longer needed? Note that for medico-legal purposes, medical records may need to be kept for many years.
- Is it clear on the face of your forms which parts a patient is obliged to complete, and which information is voluntary?
- Do you intend to offer patients a form for completion for the purpose of an application for a copy of their medical records, and have you considered the issues surrounding this option?

Disclosure and Complaint Registers

A medical practice should create a disclosure register to record disclosure of patient information made without the consent of a patient to an authorised enforcement body. It would be prudent to create a complaint register, so that if any unresolved patient complaint lead to an investigation by the Privacy Commissioner, an accurate record of the complaint and action taken can be produced. Mistakes do happen, and you should be prepared in the event of a breach of the Act.

Start a Practice Privacy Manual

Compile a manual of relevant information, index it, and make it available to all staff. It might consist of:

1. full APPs;
2. health guidelines accessible on the Privacy Commissioner's website at www.oaic.gov.au;
3. any useful fact sheets issued by the Privacy Commissioner, accessible on the above website;
4. other material produced from time to time for AMA members, accessible on the AMA's website at www.ama.com.au;
5. this Privacy and Health Record Resource Handbook;
6. sample forms from Section Five, or as developed by your practice, from which further copies can be made as required; and
7. your practice's privacy policy, website policy, information pamphlets etc.

See also Tips on Developing Privacy Policy below.

Privacy Action Plan

Do you need to appoint a privacy officer?
There is no obligation under the Act to appoint a privacy officer, and all staff need to be involved if best practice is to be achieved. However, it would be prudent to consider nominating a person to be responsible for the ongoing management of patient information. This person may be a doctor, practice manager, receptionist or someone employed specifically to perform that function. The person chosen may depend on the size of the organisation.

The person should be responsible for:

- full implementation of the practice's privacy policy;
- the handling of staff and patient privacy questions;
- the establishment of procedures to handle access requests and complaints; and
- the establishment of disclosure and complaint registers.

Develop a procedure for resolving patient complaints about your handling of their personal information
This should include establishing:

- an 'incident and complaints record' for recording complaints about the handling of personal information; and
- a 'disclosure registry' for recording disclosures made to others required under or authorised by the law without the consent of the patient.

These records will assist in the ongoing reviews of the organisation's practices to ensure adherence with the Act.

Train staff about your privacy policy and their obligations under the privacy legislation.
All staff should be familiar with the organisation's privacy policy and procedures to ensure that there are no unintentional breaches of privacy. All staff should also be aware of the patient's right to access their own information, although there may be restrictions to access. Professional staff should also have an understanding of the concepts of 'primary' and 'secondary purpose' collection in relation to patient consent for use and disclosure of their information. You may wish to provide staff members with copies of information in this resource kit of relevance to them.

Staff confidentiality agreements.
It is advisable that all staff sign a confidentiality agreement. This could be included in contracts of employment. It might include words to the effect of, '*I agree that I shall not, during the period of my employment or after its termination (however caused), disclose or use in any manner whatsoever any patient files, medical reports, or confidential knowledge gained through my employment with [name of practice]. I acknowledge that any such disclosure is in breach of privacy legislation*'. A sample confidentiality agreement is provided in Section Five.

Monitor ongoing privacy procedures to ensure compliance.
The privacy officer should regularly review and evaluate the organisation's privacy policy, and whether staff are complying with it. There may need to be changes to the policy or procedures as a result of the review, or perhaps as the result of a complaint or incident report.

Consider the need for external advice.
Some organisations may require the assistance of external providers to:

- conduct a privacy audit, develop policy and procedures, and assist in the ongoing adherence by staff; and / or
- advice as to whether additional software should be installed that records your privacy policy and your implementation procedures, allows you to monitor its working, access checklists and conduct privacy audits.

Tips on Developing a Privacy Policy

Your practice must have a privacy policy. It needs to inform patients of:

- the kinds of personal information that you collect and hold;
- how you collect and hold personal information;
- the purposes for which you collect, hold, use and disclose personal information;
- how patients may access their personal information and seek the correction of that information;
- how patients may complain about a breach of the Australian Privacy Principles and how you will deal with such a complaint; and
- whether you are likely to disclose personal information to overseas recipients; (and if so, to which countries).

Check the IT privacy of the practice

Privacy of health information applies to all communications, not just paper records. Whether communicated or transferred via the telephone, facsimile machine or e-mail, and whether stored electronically, staff must maintain privacy and confidentiality. For specific guidelines, the AMA recommends practices refer to specific documents in this area, such as the RACGP's Computer and information security standards for general practices and other office-based practices (Second edition), available at:
http://www.racgp.org.au/download/Documents/Standards/2013ciss.pdf

(Note: This is an external resource and the AMA does not warrant the accuracy of its contents.)

Some basic guidelines include ensuring:

- ☐ backup tapes or other media are stored securely or destroyed;
- ☐ anti-virus software is used for all computers with automatic updates;
- ☐ files from external sources are checked for viruses before being used;
- ☐ anti-virus updates are obtained and distributed promptly when available;
- ☐ confidential information is not sent by e-mail unless encrypted;
- ☐ e-mails are sent with a confidentiality and privilege notice;
- ☐ work-related e-mail is handled, stored and disposed of in accordance with relevant legislation;
- ☐ access privileges are granted only on a 'need to know' basis;
- ☐ there is an access approval process;
- ☐ access administration responsibilities are assigned;
- ☐ access privileges are reviewed on a periodic basis;
- ☐ contractors who require access to the system have signed confidentiality agreements;

- ☐ IT equipment is stored in secure private areas of the practice;
- ☐ there are building security measures in place;
- ☐ additional measures are taken for mobile devices;
- ☐ there is a Disaster Recovery Plan;
- ☐ there are maintenance and/or service level agreements in place for equipment and software;
- ☐ the plan contains business continuity and recovery procedures; and
- ☐ a device with electrical filtering is used to prevent damage to hardware.

Data disposal

Ensure there are procedures in place to ensure that data is removed, destroyed or cleansed once it is no longer required (particularly from floppy disks, hard drives, backup tapes, note-book computers and the like when they are no longer in use).

Information can be deleted but still be dangerous, even though a computer itself is disposed of. Data can be recovered from computers despite efforts to destroy it. Information may not be visible on the PC but it remains in the hard drive.

Consent to collection, use and disclosure of information

Consent by a patient to the collection of personal information by a medical practice is generally implied by the patient's request for a medical service. However, consent to the use and disclosure of that information is required if it is to be used and disclosed for any broader or other purpose than the main purpose for which it was collected (or any directly related purpose and within the reasonable expectations of the patient). Where information is collected in the course of providing medical care, a meeting of minds between doctor and patient is therefore required in relation to the breadth of the care envisaged.

Consideration needs to be given to how best the practice can ensure that doctor/patient expectations are aligned. Doctors should make it clear to patients how they envisage the information will be used and disclosed in the course of caring for their patient's health – whether merely for a particular episode of care, or for a more holistic approach to the patient's ongoing care. Doctors need to establish procedures for communicating this to their patients. This might be partially achieved by the provision of written patient information. In addition, clear and frank oral communication is required. In the course of the exchange, doctors must be aware of, and record, any restrictions placed by the patient on the use and disclosure of any particular personal information.

An established routine procedure to record, by a particular form of notation on a patient record, that a patient has had explained and understands and agrees to how their information is handled, is perhaps the best evidence that full consent was obtained. Doctors will appreciate that often patients sign consent forms without fully understanding what they are signing.

However, a sample consent form is provided in Section Five for adaptation, where appropriate, by medical practices, if it is required.

Access and Correction

Medical practices need to develop a policy outlining how they will handle access requests. It should include:

- who within the practice will be responsible for handling access requests;
- the fees (if any) the practice will charge for various types of access; and
- the quality standards which will be adopted in relation to proving the information in a timely manner.

Internal Privacy Manual

An internal practice manual should detail the procedures that are in place around access requests, and a method to note that the treating doctor has reviewed the material to ensure no restrictions to access or disclosure apply.

Section Five

Privacy Kit Material – Tips & Sample Forms

Getting Started Checklist

A GETTING STARTED CHECKLIST		
Checklist	**Check**	**Action / comment**
1. Have you read this resource kit and disseminated to staff where appropriate?		
2. Have you considered appointing a Privacy Officer?		
3. Have you read the 13 APPs and understood the concepts of 'primary purpose', 'secondary purpose' and 'reasonable expectations' in terms of patient consent for collection, use and disclosure of information?		
4. Have you conducted a privacy audit of your current practices and procedures?		
5. Have you conducted a security review of your current practices and procedures?		
6. Have you formulated or adopted a privacy policy with simple processes for a patient to opt out of receiving information from you?		
7. Have you developed an access request to records handling policy?		
8. Have you formulated a procedure to handle complaints or incidents regarding breaches of privacy?		
9. Have you trained your staff in relation to your organisation's privacy policy and procedures, and are they familiar with the privacy legislation?		
10. Have you developed a protocol for the ongoing review of the organisation's adherence to its privacy policy and procedures, and with privacy legislation?		

Consent Forms

The following is an example of Consent Form that may be drawn on to suit the needs of your practice. It does not replace effective oral communication between doctor and patient.

Dear (Patient Name)

COLLECTION OF PERSONAL INFORMATION, PRIVACY ACT 1988

We require your consent to collect personal information about you. Please read this information carefully, and sign where indicated below.

This medical practice collects information from you for the primary purpose of providing quality health care. We require you to provide us with your personal details and a full medical history so that we may properly assess, diagnose and treat illnesses and be pro-active in your health care. We will also use the information you provide in the following ways:

- Administrative purposes in running our medical practice
- Billing purposes, including compliance with Medicare and Health Insurance Commission requirements
- Disclosure to others involved in your health care, including treating doctors and specialists outside this medical practice. This may occur through referral to other doctors, or for medical tests and in the reports or results returned to us following the referrals. If necessary, we will discuss this with you.

{if the practice undertakes training of students, or research activities, then the following clauses may be adopted}

- Disclosure to other doctors in the practice, locums and by Registrars attached to the practice for the purpose of patient care and teaching. Please let us know if you do not want your records accessed for these purposes, and we will note your record accordingly.
- Disclosure for research and quality assurance activities to improve individual and community health care and practice management. You will be informed when such activities are being conducted and given the opportunity to "opt out" of any involvement

……

I have read the information above and understand the reasons why my information must be collected. I am also aware that this practice has a privacy policy on handling patient information.

I understand that I am not obliged to provide any information requested of me, but that my failure to do so might compromise the quality of the health care and treatment given to me.

I am aware of my right to access the information collected about me, except in some circumstances where access might legitimately be withheld. I understand I will be given an explanation in these circumstances. I understand that if I request access to information about me, the practice will be entitled to charge me fees to cover

- time spent by administrative staff to provide access at the employee's hourly rate of pay
- time necessarily spent by a medical practitioner to provide access at the practitioner's ordinary sessional rate and
- for photocopying and other disbursements at cost

I understand that if my information is to be used for any other purpose other than set out above, my further consent will be obtained.

I consent to the handling of my information by this practice for the purposes set out above, subject to any limitations on access or disclosure that I notify this practice of.

Signed:..... Date:.....
Patient

Tips on providing access to patients

- ☐ Patient access should be supervised to ensure no removal, deletion or alteration of records. They should not photocopy their own records. Although this may save staff costs and time it may raise public liability and other privacy issues. While patients are granted access to their files under the privacy legislation, ownership of the records remains with the doctor or medical practice.
- ☐ Access to patient records should not be granted without specific authorisation from the treating doctor or privacy officer. For straightforward requests, immediate access should only be given with the approval of the treating doctor or privacy officer.
- ☐ If the privacy officer is not a medical practitioner, a medical practitioner should review the record before granting access to it.
- ☐ Generally access should be granted in the form requested.
- ☐ Administrative staff should not make decisions on whether access should be granted or not. All requests should be referred to the treating doctor or privacy officer.
- ☐ Written requests are not required by the legislation. However, in complex cases, it may be prudent to require that the request be made in writing, as the request should be noted on file for future reference.
- ☐ Access should be given within 30 days of receipt of request, in most circumstances.
- ☐ Administrative charges to cover the cost of complying with the request should be reasonable. Routine tasks, such as photocopying, should be done by administrative staff, and charged accordingly.

Sample Access Request Form

This form may be used when individuals request access to medical records. It should be used in conjunction with the Processing Access Requests Information Sheet contained in this Resource Handbook.

Access Request Form

Name of Person seeking Access:……..

Name on Medical Record/Name of Patient:……

Relationship between person seeking access and patient:……

Medical Records required:……

……

……

(eg. pathology test results, whole file, records relating to treatment for (insert condition), records between (insert relevant dates) etc)

Form of Access required:……

……..

……..

(for example: photocopy, summary, viewing, explanation etc)

Records to be: ☐ collected on _____/_____/20 ___.

☐ posted to: ……..

……

……..

Costs

No charge will be made to lodge this request for access. However, in providing access to you, this practice may incur charges arising out of: retrieval of records from archives, doctor's time to peruse the records, photocopy charges and doctor's time for explanation (which is not Medicare or private health insurance funded).

The practice may charge fees to cover

- *time spent by administrative staff to provide access at the employee's hourly rate of pay*
- *time necessarily spent by a medical practitioner to provide access at the practitioner's ordinary sessional rate and*
- *for photocopying and other disbursements at cost.*

If you have any queries regarding the costs of your request for access, please discuss these with us.

Please Note: In some cases, access to medical records may be restricted due to specified circumstances in the Privacy Act. If your request falls within one of these stated exceptions, we will provide you with an explanation as to why access could be granted, and to discuss if there is another alternative that will meet your requirements

_____

Office Use Only

Acknowledgment of access request provided ☐
Costs of access discussed ☐

Access granted / denied

Records provided on _____/_____/20____ by ……

Signature of Privacy Officer/Doctor

Confidentiality Agreement

This is an example of a Confidentiality Clause that might be included in or accompany a contract of employment of staff of a medical practice.

Privacy Clause

Dear **[Insert name of employee]**

As an employee of **[insert name of employer practice or organisation]** I agree that I will abide by the privacy policy, privacy legislation and privacy procedures which apply to this **[practice or organisation]**. In particular, I agree that:

(a) I shall not, during my period of employment with **[insert name of employer practice or organisation]**, disclose or use any patient files, medical reports or confidential knowledge obtained through my employment with **[insert name of employer practice or organisation],** other than to perform my usual duties of employment as authorised and detailed above **[assuming that duty statement is included in employment agreement]** or specifically requested by my supervisor to perform.

(b) Any breach of this **[practice or organisation]**'s privacy policy or privacy legislation, caused by me, whether intentional or not, may result in disciplinary action, including immediate termination.

(c) The obligations contained in clauses (a) to (b) will continue even after the termination of my employment with **[insert name of employer practice or organisation]**, whatever the reason for the termination.

(d) Upon termination of my employment with [insert name of employer practice or organisation], for whatever reason, I will immediately deliver to **[name of practice or organisation]** all patient files, medical reports or other documents which are in my possession or under my control which in any way relate to the business of **[insert name of practice or organisation]** or its patients past or present.

Signed: …….. Date: ……./……./……

Sample Privacy Policy

Please see supplementary document at:

https://ama.com.au/article/privacy-and-health-record-resource-handbook-medical-practitioners-private-sector

AMA Sample Privacy Policy

Sample Privacy Policy

[***Note:*** you should provide the privacy policy on your website and have a physical hard copy on display and have copies available upon request]

DISCLAIMER: This sample may be used as the basis for a privacy policy, but it is a guide only and needs to be carefully worded to suit the individual practice. It is not intended to be a complete privacy policy, only the basis for one. The AMA is not responsible for any breaches of privacy or alleged breaches of privacy arising out of the use of this template.

A NOTE FOR PRACTICES: Where we have A '***Note***' in brackets

[…], in orange font this is intended as a note for your information and is not intended to be part of the text of the policy.

Sample Privacy Policy [***Note:*** you may wish to state the version number and date of the policy, to ensure you keep your policy current. You should review your policy regularly to ensure compliance with the Privacy Act. Anytime you change the way you handle personal information you need to review your policy to ensure that it still accurately reflects your procedures]

XXXX Medical Practice Privacy Policy [***Note*****:** Make it clear whether you are referring to one sole practice or a practice which is part of a larger entity or group of practices.]

1. Introduction

Our practice is committed to best practice in relation to the management of information we collect. This practice has developed a policy to protect patient privacy in compliance with the Privacy Act 1988 (Cth) ('the Privacy Act'). Our policy is to inform you of:

- the kinds of information that we collect and hold, which, as a medical practice, is likely to be 'health information' for the purposes of the Privacy Act;
- how we collect and hold personal information;
- the purposes for which we collect, hold, use and disclose personal information;
- how you may access your personal information and seek the correction of that information;
- how you may complain about a breach of the Australian Privacy Principles and how we will deal with such a complaint;
- whether we are likely to disclose personal information to overseas recipients;

[***Note***: APP entities such as medical practices are required to inform patients whether or not they are likely to disclose personal information to overseas recipients]

2. What kinds of personal information do we collect?

The type of information we may collect and hold includes:

- Your name, address, date of birth, email and contact details

- Medicare number , DVA number and other government identifiers, although we will not use these for the purposes of identifying you in our practice
- Other health information about you, including:
    - notes of your symptoms or diagnosis and the treatment given to you
    - your specialist reports and test results
    - your appointment and billing details
    - your prescriptions and other pharmaceutical purchases
    - your dental records
    - your genetic information
    - your healthcare identifier
    - any other information about your race, sexuality or religion, when collected by a health service provider.

3. How do we collect and hold personal information?

We will generally collect personal information:

- from you directly when you provide your details to us. This might be via a face to face discussion, telephone conversation, registration form or online form
- from a person responsible for you
- from third parties where the Privacy Act or other law allows it - this may include, but is not limited to: other members of your treating team, diagnostic centres, specialists, hospitals, the My Health Record system[1], electronic prescription services, Medicare, your health insurer, the Pharmaceutical Benefits Scheme

4. Why do we collect, hold, use and disclose personal information?

In general, we collect, hold, use and disclose your personal information for the following purposes:

- to provide health services to you
- to communicate with you in relation to the health service being provided to you [***Note*** re direct marketing: –sensitive information can only be used for direct marketing if consent has been given. Consent may be implied in certain circumstances. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the practice. If you do intend to communicate with patients via direct marketing with their consent, make it clear that the patient may opt out of direct marketing at any time by notifying your practice, and let them know they can do that by sending the practice a letter or email and provide the contact details for them to do so. The AMA recommends caution in relation to direct marketing and medical practices, and you may like to seek independent advice before engaging in direct marketing with patients].
- to comply with our legal obligations, including, but not limited to, mandatory notification of communicable diseases or mandatory reporting under applicable child protection legislation.

[1] See: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home

- to help us manage our accounts and administrative services, including billing, arrangements with health funds, pursuing unpaid accounts, management of our ITC systems
- for consultations with other doctors and allied health professional involved in your healthcare;
- to obtain, analyse and discuss test results from diagnostic and pathology laboratories
- for identification and insurance claiming
- [***Note***: If your practice uses the My Health Record system]: If you have a My Health Record, to upload your personal information to, and download your personal information from, the My Health Record system.
- [***Note***: If your practice uses an electronic transfer of prescriptions service - you will need to specify if your practice participates in this service]: Information can also be disclosed through an electronic transfer of prescriptions service.
- To liaise with your health fund, government and regulatory bodies such as Medicare, the Department of Veteran's Affairs and the Office of the Australian Information Commissioner (OAIC) (if you make a privacy complaint to the OAIC), as necessary.

5. How can you access and correct your personal information?

You have a right to seek access to, and correction of the personal information which we hold about you. [***Note***: If a fee is charged for providing access, you will need to advise patients of the cost in advance].

For details on how to access and correct your health record, please contact our practice as noted below under 'Contact Details': [***Note***: See below under 'Contact Details']

We will normally respond to your request within 30 days.

6. How do we hold your personal information?

Our staff are trained and required to respect and protect your privacy. We take reasonable steps to protect information held from misuse and loss and from unauthorised access, modification or disclosure. This includes:

[***Note***: you should provide some detail about how you hold your patients' health information. You need to provide information on the most relevant security measures you have in place. Without jeopardising security, your policy should describe some of the security processes that the practice applies – for example strong password protections applied; access to personal information restricted on a 'need to know' basis', paper files kept in locked cabinets etc. Some examples might also include:

- Holding your information on an encrypted database
- Holding your information in secure cloud storage (you can explain whether this information is encrypted or what other security measures are taken with third party storage)
- Holding your information in a lockable cabinet
- Our staff sign confidentiality agreements
- Our practice has document retention and destruction policies]

7. Privacy related questions and complaints

If you have any questions about privacy-related issues or wish to complain about a breach of the Australian Privacy Principles or the handling of your personal information by us, you may lodge your complaint in writing to (see below for details). We will normally respond to your request within 30 days.

If you are dissatisfied with our response, you may refer the matter to the OAIC:

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Fax: +61 2 9284 9666

Post: GPO Box 5218

Sydney NSW 2001

Website: https://www.oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint

8. Anonymity and pseudonyms

The Privacy Act provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with our practice, except in certain circumstances, such as where it is impracticable for us to deal with you if you have not identified yourself.

[***Note:*** This is up to the individual practice, but the AMA is of the view that in medical practices it is largely impracticable to deal with patients anonymously or via a pseudonym. The provision of medical services is likely to be impacted, and billing via Medicare or a health insurer where applicable is likely to be impracticable. Of course, in some instances a patient seeking certain treatments may be prepared to forego notifying their insurer or seeking a Medicare benefit and pay the practice direct. It up to the practice to have a policy to follow to determine whether this is impracticable or not.]

9. Overseas disclosure.

[*Note*: If personal information is likely to be disclosed to overseas recipients, the countries in which such recipients are likely to be located must also be specified if it is practicable to do so. If you will not be disclosing information overseas or it is unlikely that you will do so, your policy should note this. If you do intend to do so, you must make a clear statement such as the one below:]

We may disclose your personal information to the following overseas recipients:

- any practice or individual who assists us in providing services (such as where you have come from overseas and had your health record transferred from overseas or have treatment continuing from an overseas provider) [***Note***: in this case, it is likely that you will have the patient's permission for the disclosure, but it is best to check that the terms of the permission you have cover this eventuality.]
- overseas transcription services [***Note:*** if you use a transcription service, you should insert what is being transcribed, such as your clinical notes, etc.]

  overseas based cloud storage [***Note***: you need to be aware that privacy and cloud based storage services can be a complex issue. For example, if you use an overseas based cloud-storage service provider but the information is encrypted to the point where the cloud

service provider cannot access it, but merely stores it, then it is likely that the practice will be considered to be holding and using that personal information and not disclosing it to the cloud service provider. However, if the cloud service provider can access and collect the information, this is likely to be an overseas 'disclosure' on the part of the practice. If in doubt, it is best to consider the use of cloud based storage services as a 'disclosure'. For more information, see: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information]

- anyone else to whom you authorise us to disclose it

10. Updates to this Policy

This Policy will be reviewed from time to time to take account of new laws and technology, changes to our operations and other necessary developments. Updates will be publicised on the practice's website.

[***Note***: If your practice does not have an online presence or if you have many patients who do not have internet access you may consider the following sentence instead - "A notification of the updates to the policy will be displayed at our reception desk".]

11. Privacy and websites

[***Note***: the policy should ordinarily be made available on your practice's website if you have one. If your practice has a website, you should consider adding details about collecting personal information via the practice's website or when you interact with patients online (eg through social media or by email), as well as details regarding your practice's collection of personal information through the use of website analytics, cookies, etc. You should also note that how your practice's website operates, for example whether it allows for patient feedback, links to social media or whether it allows for appointments to made online. Alternatively, you may consider a separate website related policy that covers these issues.]

12. Contact details for privacy related issues

[***Note***: insert name, telephone number and email address or postal address of privacy contact officer here. For the purposes of this provision your practice may create a generic 'privacy@...' email address to ensure that regardless of staff turnover, access and correction requests will always be properly received].

Standards for general practices 4.2.1

Standards for general practices (4th edition)

including Interpretive guide for Aboriginal and Torres Strait Islander health services

Standard 4.2 Management of health information

Our practice has an effective system for managing patient information.

Criterion 4.2.1

Confidentiality and privacy of health information

Our practice collects personal health information and safeguards its confidentiality and privacy in accordance with Australian Privacy Principles.

Indicators

► A. Our practice team can describe how we ensure the confidentiality of patient health records.

► B. Our practice team can demonstrate how patient health records can be accessed by an appropriate team member when required.

► C. Our practice team can describe the processes we use to provide patients with access to their health information.

► D. Our practice team can demonstrate how patients are informed about our practice's policy regarding management of their personal health information.

► E. Our practice team can describe the procedures for transferring relevant patient health information to another service provider.

► F. Our practice team can demonstrate how we facilitate the timely, authorised and secure transfer of patient health information in relation to valid requests.

► G. When we collect patient health information for quality improvement or professional development activities, we only transfer identified patient health information to a third party once informed patient consent has been obtained. *Amended in May 2013.*

► H. Whenever any member of our practice team is conducting research involving our patients, we can demonstrate that the research has appropriate approval from an ethics committee.

Explanation

Key points

- Privacy of health information is a legislative requirement
- The practice needs to have a documented privacy policy for the management of patient health information
- Patients need to be informed about the practice's privacy policy
- *Guidelines on Australian Privacy Principles* will assist general practices to meet their legal obligations in relation to the collection, use and disclosure of health information.

Personal information and health information

The Privacy Act 1988 applies to personal information. Health information is a particular subset of personal information and can include any information collected to provide a health service, such as a person's name, address, account details, Medicare number and any health information such as a medical or personal opinion about a person's health, disability or health status.

Sometimes details about a person's medical history or other contextual information such as details of an appointment can identify them, even if no name is attached to that information. This is still considered health information and as such it must be protected under the Privacy Act 1988.

Australian Privacy Principles

In March 2014, privacy law reforms introduced the Australian Privacy Principles (APPs) into the Privacy Act 1988. The APPs regulate the handling of personal information by both Australian government agencies and some private sector organisations. The reforms compliment the culture of confidentiality that exists in general practice.

Practices should familiarise with the APPs, including the Australian Privacy Principle Guidelines published by the Office of the Australian Information Commissioner. The Guidelines are available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines (http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines)

RACGP Handbook

The RACGP *Handbook for the management of health information in general practice* (3rd edition) provides further information about safeguards and procedures required by general practices in order to meet appropriate legal and ethical standards concerning the privacy and security of patient records.

RACGP Computer and Information security standards (CISS)

'Compliance indicators for the Australian Privacy Principles' is an addendum to the *Computer and information security standards* (2nd edition) (CISS)and is designed to assist general practice to meet its legal obligations of the APPs. CISS provides a brief explanation of each APP requirement and the steps general practices need to take to ensure compliance.

State privacy legislation

As well as being familiar with the APPs, practices need to be familiar with the relevant state/territory privacy and health records legislation (where relevant) as this will also impact on the way in which practices manage patient health information. For more information visit www.oaic.gov.au or the local state equivalent.

Practice privacy policy

The RACGP has developed a privacy policy template for general practices to assist compliance with the requirements of the APPs. The template is titled the *APP privacy policy: managing patient health information*.

Communicating with patients

A practice's privacy policy can be made available to patients in a number of ways including a sign at reception, a separate brochure and a section of the patient information sheet or a notice/link on the practice website.

The Privacy Act 1988 sets out two compulsory mechanisms for informing patients about how their health information will be used.

1. A practice privacy policy. Organisations are required to provide this policy on request and commonly satisfy this requirement by making their privacy policy available on their website or on a sign at reception.
2. A 'collection statement' which contains prescribed information, including the following:

- the identity of the practice and how to contact it
- the fact information is collected and the circumstances of that collection
- the fact that patients can access their own heath information
- the purpose for which the information is collected
- other organisations to which the practice usually discloses patient health information
- any law that requires the particular information to be collected
- the main consequence for the individual if important health information is not provided
- the existence of a supporting privacy policy.

Patient consent

Patient consent should be obtained at an early stage in the process of clinical care. It is important to distinguish between consent to treatment and consent to the handling of patient health information even if such consent processes happen to occur at the same time.

Consent may be written (ideal) or verbal, and may be provided by way of:

- express consent, such as where the patient signs or clearly articulates their agreement
- implied (or inferred) consent, where the circumstances are such to reasonably infer the patient has consented.

Transfer of health information

The correct process for transferring patient health information to others, such as other health service providers or in response to third party requests, is outlined in section 2 'Use and Disclosure' in the OFPC *Guidelines on Privacy in the Private Health* Sector. Practices are advised to contact their insurers if they have any concerns about third party requests for the transfer of patient health information.

Research

Research is an important component of general practice in Australia. Practices are encouraged to participate in research both within their own practice and through reputable external bodies.

If a practice is using de-identified patient health information, there are still some situations in which a practice should obtain informed patient consent, and some situations where informed patient consent is not required. Consent requirements, when using de-identified data, will be decided by a Human Research Ethics Committee.

Further information about research in general practice, including the requirements for ethics approval, can be found in the National Health and Medical Research Council's (NHMRC) *National statement on ethical conduct in human research* available at www.nhmrc.gov.au/_files_nhmrc/file/publications/synopses/e72-jul09.pdf (http://www.nhmrc.gov.au/_files_nhmrc/file/publications/synopses/e72-jul09.pdf)

Quality improvement

For a quality improvement activity to be undertaken within a general practice, where the primary purpose is to monitor, evaluate or improve the quality of healthcare delivered by the practice, ethics approval is not required.

Clinical audits using a tool such as the Clinical Audit Tool (CAT) (see Criterion 3.1.1 Quality improvement activities) or 'plan, do, study, act' cycles undertaken within a general practice as part of a quality improvement activity do not require ethics approval. For example, a practice wishing to determine how many of its pregnant patients are given advice on smoking cessation, or how many patients with heart failure are prescribed ACE inhibitors and beta blockers, may complete an audit on their practice data.

In general, a practice's quality improvement or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment or service would not be considered a directly related secondary purpose for information use or disclosure. In other words, it is likely the practice would need to seek specific consent for this use of patients' health information for clinical audit activities.

To ensure patients understand and have reasonable expectations of quality improvement activities, practices are encouraged to include information about quality improvement activities and clinical audits in the practice policy on managing health information. Ideally, express consent for these activities will be obtained upon patient registration.

Disclosure of health information to carers

The disclosure of necessary health information by an organisation to an individual's responsible person (such as a carer) is permitted by the Privacy Act 1988, providing it is reasonably necessary, in the context of providing a health service to that individual and the individual is physically or legally incapable of consenting or communicating that consent. If a

situation arises where a carer is seeking access to a patient's health information, practices are encouraged to contact their medical defence organisation for advice before such access is granted.

Practice closures

The correct process for handling patient health information on the closure of a practice can be accessed from the Office of the Australian Information Commissioner at www.oaic.gov.au (http://www.oaic.gov.au)

See also

- Criterion 1.7.1 Patient health records (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-services/1-7/patient-health-records/)

4.1.2 Occupational health and safety (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-1/occupational-health-and-safety/)
◄ PREVIOUS (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-1/occupational-health-and-safety/)

4.2.2 Information security (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/information-security/)
NEXT ► (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/information-security/)

Standards for general practices 4.2.2

Standards for general practices (4th edition)

including Interpretive guide for Aboriginal and Torres Strait Islander health services

Standard 4.2 Management of health information

Our practice has an effective system for managing patient information.

Criterion 4.2.2

Information security

Our practice ensures the security of our patient health information.

Indicators

► A. Our practice team can demonstrate that the personal health information of patients of our practice is neither stored, nor left visible, in areas where members of the public have unrestricted access or where constant staff supervision is not easily provided.

► B. Our practice ensures that our practice computers and servers comply with the RACGP computer security checklist and that:

- computers are only accessible via individual password access to those in the practice team who have appropriate levels of authorisation
- computers have screensavers or other automated privacy protection devices are enabled to prevent unauthorised access to computers
- servers are backed up and checked at frequent intervals, consistent with a documented business continuity plan
- back up information is stored in a secure off site environment
- computers are protected by antivirus software that is installed and updated regularly
- computers connected to the internet are protected by appropriate hardware/software firewalls.

► C. If our practice uses computers to store personal health information, we have a business continuity plan that has been developed, tested and documented.

► D. Our practice has a designated person with primary responsibility for the practice's electronic systems and computer security.

► E. Our communication devices are accessible only to authorised staff.

► F. Electronic data transmission of patient health information from our practice is in a secure format.

► G. Our practice has an appropriate method of destroying health record systems before disposal (eg. shredding of paper records, removal and reformatting of hard drives).

Explanation

Key points

- The privacy and security of health information held by a practice is a legal obligation
- Computer security is an important aspect of information security
- Information security must encompass availability of information, integrity of information and designated access to information
- Computerised practices need a contingency plan to cover computer crashes
- The practice needs a designated staff member with primary responsibility for computer security.

RACGP resources

The RACGP Computer and Information Security Standards (CISS) (http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/) and accompanying workbook will provide guidance on the essential information needed to put in place effective computer and information security. The workbook, when completed by practice staff, will form part of the general practice's policies and procedures manual. The computer and information security checklist provides a record of the 12 basic computer and information security categories that should be undertaken.

Computer security

It is important to have a designated member of the practice team with responsibility for computer security.

This person needs to know who and when to call for expert advice, educate staff on data security and ensure security protocols are followed. The contact details of any external expert used by the practice need to be available to other relevant practice staff.

Business continuity plan

When a practice uses computers to store patient health information, the practice needs to have a sound backup system and a contingency plan to protect practice information in the event of an adverse incident, such as a system crash or power failure. This plan needs to encompass all critical areas of the practice's operations such as making appointments, billing patients and collecting patient health information. Once a plan has been formulated, it needs to be tested on a regular basis to ensure backup protocols work properly.

Consideration needs to be given to the increasing portability of computer based systems. These need to be managed in an equally secure manner as the main practice network. Furthermore, being potentially more accessible to people outside the practice team, the physical security of portable equipment needs to be taken into account (eg. laptop computers, personal digital assistants [PDAs] and mobile telephones carried by GPs when travelling between different locations).

Replacing equipment with hard drive memory

The practice is advised to review the RACGP *Computer security guidelines: A self assessment guide and checklist for general practice* (3rd edition) when equipment is to be made redundant by the practice, to ensure key information is not lost or transferred inadvertently. Deleting records is insufficient to clear data from a computer system.

Practices need to be aware that other equipment such as photocopiers and fax machines may have hard drive memory and that confidential information needs to be properly removed before the practice disposes of such equipment.

Preventing unauthorised access to patient health information

It is likely that practices will have different levels of access to patient health information for different staff members and this differentiated access needs to be documented in the practice's policy and procedure manual. To protect the security of health information, GPs and other practice staff should not give their computer passwords to others in the team.

Patient health records and computer screens should be positioned so confidential information is not readily visible to anybody but the appropriate members of the practice team. Screen savers or other automated privacy protection devices should be used to prevent unauthorised access to computers in a situation like a doctor momentarily leaving the consultation room. Although the focus of this criterion is information security, it is noted that many doctors now use the computer screen as a useful tool for sharing information with patients during a consultation.

Active and inactive patient health records

The practice must ensure that both active and inactive patient health records are kept and stored securely. An inactive patient health record is generally considered to be the record of a patient who has not attended the practice/ service three or more times in the past 2 years. It is recommended that inactive patient health records are retained by the practice indefinitely

or as stipulated by the relevant national, state or territory legislation. General practices may want to consult their GPs' medical defence organisations when deciding on the practice's policy with respect to the retention of records.

Changes to computer hardware and software over time may prevent older versions of medical software from running correctly on newer systems and provision needs to be made for this eventuality, which may include retaining older systems for record storage purposes.

4.2.1 Confidentiality and privacy of health information (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/confidentiality-and-privacy-of-health-information/)

◄ PREVIOUS (http://www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/confidentiality-and-privacy-of-health-information/)

5.1.1 Practice facilities (http://www.racgp.org.au/your-practice/standards/standards4thedition/physical-factors/5-1/practice-facilities/)

NEXT ► (http://www.racgp.org.au/your-practice/standards/standards4thedition/physical-factors/5-1/practice-facilities/)

Guide to securing personal information "Office of the Australian Information Commissioner"

Australian Government

Office of the Australian Information Commissioner

Guide to securing personal information

'Reasonable steps' to protect personal information

January 2015

Contents

Introduction 2
The Privacy Act, the APPs, and other obligations 2
Other information security resources 4
What is personal information security? 5
Personal information security 5
Why is it important? 6
The information lifecycle 7
1. Consider whether to collect personal information 8
2. Privacy by design 8
3. Assessing the risks 9
4. Taking appropriate steps and putting into place strategies to protect personal information 10
5. Destroy or de-identify personal information 11
Part A — Circumstances that affect assessment of reasonable steps 12
Nature of the entity 12
Amount and sensitivity of personal information held 13
Adverse consequences for an individual 14
Practicality of implementation 15
Privacy invasiveness 15
Part B — Steps and strategies which may be reasonable to take 16
Governance, culture and training 17
Internal practices, procedures and systems 20
ICT security 21
Access security 27
Third party providers (including cloud computing) 33
Data breaches 36
Physical security 36
Destruction or de-identification of personal information 37
Standards 39
Appendix A — Glossary of terms 41
Appendix B — Additional resources 43
OAIC resources 43
Other resources 43

Introduction

This 'Guide to securing personal information' (Guide) provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* (Cth) (Privacy Act) to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. It also includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once it is no longer needed (unless an exception applies).

This guide is intended for use by entities covered by the Privacy Act, including organisations, agencies, credit reporting bodies (CRBs), credit providers and tax file number recipients.[1] However, this guide may also be relevant to organisations not subject to the Privacy Act as a model for better personal information security practice.

This guide is not legally binding. However, the Office of the Australian Information Commissioner (OAIC) will refer to this guide when undertaking its Privacy Act functions, including when investigating whether an entity has complied with its personal information security obligations (s 40) or when undertaking an assessment (s 33C). Information on when and how we might exercise our regulatory powers is available in the OAIC's *Privacy Regulatory Action Policy*.

Entities subject to the Privacy Act should read this guide in conjunction with the *Australian Privacy Principles guidelines* (APP guidelines). The APP guidelines outline the mandatory requirements of the Australian Privacy Principles (APPs), how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.

The introductory sections of this guide include a discussion of what is personal information security, why you should have it, and how you should protect personal information through the stages of its lifecycle. Part A discusses five general circumstances that affect what steps an entity should take to protect personal information. Under nine broad topics, Part B outlines examples of key steps and strategies you should consider taking to protect personal information including a number of questions you should ask yourself when considering or implementing these steps or strategies.

This guide assumes some knowledge of privacy and security concepts. Additional information and resources is available in Appendix B.

The Privacy Act, the APPs, and other obligations

The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government (and Norfolk Island) agencies (APP entities).

[1] For more information on the jurisdiction of the Privacy Act, see our 'Who is covered by privacy' webpage. We have used the term 'entity' throughout this guide to refer to all agencies and organisations subject to one or more of the provisions of the Privacy Act.

APP 11 requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information.[2]

Specifically, APP 11.1 states that an APP entity that holds personal information must take reasonable steps to protect the information from **misuse**, **interference** and **loss**, as well as **unauthorised access**, **modification** or **disclosure.**[3]

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[4] This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.[5]

An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'.[6] The term 'holds' extends beyond physical possession to include a record that an entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, 'holds' that personal information.[7]

When considering the security of personal information you also need to be mindful of other obligations under the Privacy Act, such as your obligations under APP 8 (Cross-border disclosure of personal information) and APP 12 (Access to personal information).

Other obligations

All entities will also need to be aware of relevant legislation (other than the APPs) that impose other obligations in relation to personal information security.

If you are a credit reporting body or credit provider covered by Part IIIA of the Privacy Act and the registered CR code;[8] a tax file number recipient covered by the *Tax File Number Guidelines 2011*; or a health care provider covered by the *Personally Controlled Electronic Health Records Act 2012* or the *Healthcare Identifiers Act 2010* you may have additional personal information security obligations.

---

[2] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p 86.

[3] The six terms listed in APP 11, 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure', are not defined in the Privacy Act. See Chapter 11 of the APP guidelines for further guidance on the meaning of these terms.

[4] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.

[5] For more information on destroying or de-identifying personal information see Chapter 11 of the APP guidelines.

[6] See s 6(1) of the Privacy Act.

[7] See APP guidelines Chapter B: Key concepts.

[8] See ss 20Q and 21S of the Privacy Act and cl. 15 of the registered CR code. The provisions in Part IIIA make it clear whether the obligations in Part IIIA replace relevant APPs or apply in addition to relevant APPs. For example, s 21S states that if a credit provider is an APP entity, APP 11 does not apply to them in relation to credit eligibility information.

Under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), Australian Government agencies must also act in a way that is not inconsistent with the policies of the Australian Government.[9] From the security perspective these policies include the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government.

Other information security resources

The advice provided in this guide is not intended to be exhaustive and it does not seek to replace any existing government or industry resources regarding information security. Compliance with these resources may be a relevant consideration in meeting the Privacy Act's requirements for personal information security.

Resources related to personal information security are widely available and entities should be aware of any relevant government, industry or technology specific standards, guidance, frameworks or obligations and incorporate these into their information security practices. A list of additional resources is at Appendix B.

[9] Under s 21 of the PGPA Act the accountable authority of a non-corporate Commonwealth entity must govern the entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government. Paragraph 15(1)(a) is about promoting the proper use and management of public resources for which the accountable authority is responsible.

What is personal information security?

Section 6 of the Privacy Act defines 'personal information' as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable.[10] This might include a person's name and address, medical records, bank account details, photos, videos and even information about what an individual likes, their opinions and where they work.

An important subset of personal information in the Privacy Act is 'sensitive information.' Sensitive information is defined in the glossary, and includes health information.[11] The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information.

Whether information constitutes personal information under the Privacy Act will depend on whether an individual can be identified or is 'reasonably identifiable' in the particular circumstances.

Some information may not be personal information when considered on its own. However, when combined with other information held or available to you, it may become 'personal information'. These pieces of information may be collected by, or become available to, you at different times. Whether an individual is 'reasonably identifiable' from that information will depend on a range of factors, including the time and cost that would be involved in re-identifying them.

It is essential that you are able to recognise the dynamic nature of information, and that information can become personal information sometime after you have collected it. You should be fully aware of the personal information you handle, where it is kept and the risks associated with that information. If it is unclear whether an individual is 'reasonably identifiable' you should err on the side of caution and treat the information as personal information.

Personal information security

'Information security' involves all measures used to protect any information generated by an entity or individual, that is not intended to be made publicly available, from compromise, loss of integrity or unavailability.[12] This can include personal information, security classified information and commercially confidential information.

'Personal information security' is the main focus of this guide and specifically relates to entities taking reasonable steps to protect personal information (including sensitive information) from misuse, interference and loss, as well as unauthorised access,

[10] The full definition of 'Personal information' is set out in the Glossary section.

[11] For more detail on the definition of 'personal information' and 'sensitive information' see the APP guidelines Chapter B: Key concepts.

[12] Australian Signals Directorate, *Australian Government Information Security Manual,* Controls manual, Glossary of Terms – definition of information security, p.314.

modification or disclosure. This will include consideration of matters before you collect personal information, including whether you should collect it at all.

Why is it important?

Personal information security is about more than just ensuring compliance with the requirements of the Privacy Act. If you mishandle the personal information of your customers, it can cause a financial or reputational loss to the customer. In turn, this can also lead to a loss of trust and considerable harm to your reputation. A significant breach may result in a loss of customers or business partners and revenue.

If personal information that is essential to your functions or activities is lost or altered, it can have a serious impact on your ability to undertake business as usual.

The benefits of applying personal information security to your business practices can include more efficient processes. It also reduces the risk of privacy breaches and the time and resources involved in addressing any breaches that do occur.[13]

Many of the steps and strategies in this guide will also assist you to take reasonable steps to ensure good handling of other types of information, such as commercially confidential information.

[13] Certain organisations such as the Ponemon Institute (www.ponemon.org) have sought to quantify the cost of data breaches to business. In its 2014 Cost of Data Breach Study: Australia, Ponemon found the average data breach cost to a company to be $2.8m. A copy of the report can be found on the IMB website or on the Computerworld website. Note registration is required to access the report.

The information lifecycle

If you handle personal information, you should consider how you will protect personal information during the stages of its lifecycle.

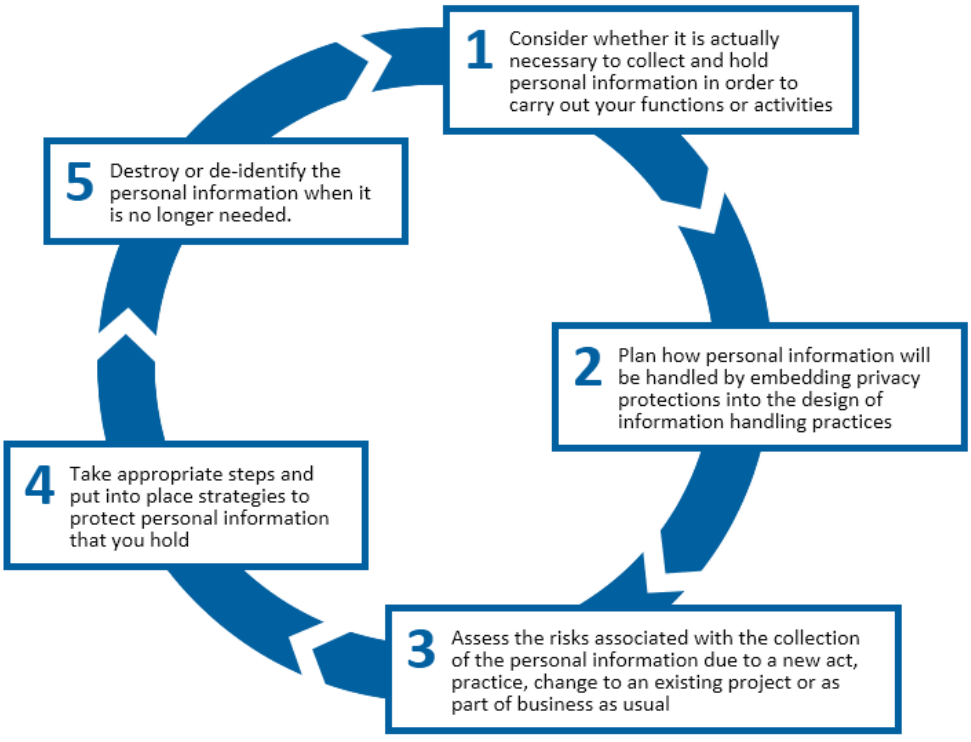
Personal information security throughout the lifecycle involves:

1. considering whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities
2. planning how personal information will be handled by embedding privacy protections into the design of information handling practices
3. assessing the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual
4. taking appropriate steps and putting into place strategies to protect personal information that you hold
5. destruction or de-identification of the personal information when it is no longer needed.

To effectively protect personal information throughout its lifecycle, you will need to be aware of when and how you are collecting it and when and how you hold it. As noted above, your personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

Additionally, the lifecycle may include the passing of personal information to a third party for storage, processing or destruction.

The information lifecycle



1. Consider whether to collect personal information

Under APP 3, you should only collect personal information that is reasonably necessary (and for agencies, directly related) to carry out your functions or activities. Over-collection can increase risks for the security of personal information.

Therefore, the first step in managing the security of personal information is to ask whether the collection of personal information is reasonably necessary to carry out your functions or activities.[14] If it is, you should then consider, even if you can collect it, should it be collected? That is, do you really need to collect the personal information or can the collection be minimised?

Personal information that is not collected or is not stored cannot be mishandled.

2. Privacy by design

APP 1 outlines the requirements for APP entities to manage personal information in an open and transparent way. This includes taking reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. The OAIC refers to this as 'Privacy by design'. Privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes, in line with APP1.

You should design your personal information security measures with the aim to:

- prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information
- detect privacy breaches promptly
- be ready to respond to potential privacy breaches in a timely and appropriate manner.

You will be better placed to meet your personal information security obligations if you embed them early, including by choosing the appropriate technology and by incorporating measures that are able to evolve to support the changing technology landscape over time. You also need to take into account the rapid development of new and existing technologies and platforms when designing your information security policies and systems.

An important element of 'privacy by design' is to integrate privacy into your risk management strategies (see 'Assessing the risks' below). Robust internal personal information-handling practices, procedures and systems can assist you to embed good personal information handling practices and to respond effectively in the event a privacy breach occurs.

[14] For agencies it can also be collected if it is 'directly related' to its functions or activities.

3. Assessing the risks

Assessing the security risks to personal information is also an important element of 'privacy by design'. You can assess your personal information security risks by conducting a privacy impact assessment (PIA), an information security risk assessment and regular reviews of your personal information security controls. You should use PIAs and information security risk assessments along with regular reviews so that you are aware of the variety of security risks you face, including threats and vulnerabilities, along with the possible impacts before designing and implementing your personal information security framework. They will also assist you in integrating privacy into your risk management strategies.

PIAs

A PIA is a written assessment that identifies the privacy impacts of a proposal and sets out recommendations for managing, minimising or eliminating those impacts. Generally, a PIA should:

- describe the personal information flows in a proposal
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

A PIA, especially one conducted at the early stage of a proposal's development, can assist you to identify any personal information security risks and the reasonable steps that you could take to protect personal information. A PIA can also be seen as an iterative process during the life of any proposal, being updated to take account of changes to the proposal as it evolves.

A detailed guide to conducting PIAs is available from the OAIC website. The OAIC encourages entities to undertake a PIA for any new proposals across all business activities that involve the handling of personal information.[15] The PIA guide includes a threshold assessment to assist you in determining whether it is appropriate for you to undertake a PIA. It will depend on a proposal's size, complexity and scope and the extent to which it involves personal information.

While the PIA guide focuses on undertaking PIAs for new projects, you should also consider applying the same principles across your business generally, including existing business operations, to give a greater understanding of the privacy risks that exist currently. Entities should also consider building the use of PIAs into their risk management processes and plans.

[15] Under s 33D of the Privacy Act, if an agency proposes to engage in an activity or function involving the handling of personal information and if the OAIC considers that the activity or function might have a significant impact on the privacy of individuals, the OAIC may direct the agency to give the OAIC, within a specified period, a PIA about the activity or function.

Information security risk assessments

You may also need to conduct an information security risk assessment (also known as a threat risk assessment) in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA because it involves the identification and evaluation of security risks, including threats and vulnerabilities, and the potential impacts of these risks to information (including personal information) handled by an entity. As with a PIA, an information security risk assessment can be seen as an iterative process and may be undertaken across your business generally.

The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.

Once the risks have been identified, you should then review your information security controls (virtual and physical) to determine if they are adequate in mitigating the risks. Given that processes, information, personnel, applications and infrastructure change regularly, and given the constantly evolving technology and security risk landscape, regular review and monitoring of personal information security controls is crucial.

Risk of human error

Threats to personal information can be internal or external as well as malicious or unintentional. Privacy breaches can arise as a result of human activity or events such as natural disasters. Human error is regularly claimed as the cause of privacy incidents; however entities should assume that human error will occur and design for it.[16] Research has shown that human error can be seen as a trigger rather than a cause of an incident.[17] PIAs, information security risk assessments and regular reviews will enable you to design practices, procedures and systems to deal with the foreseeable risk of human error and minimise its effect.

4. Taking appropriate steps and putting into place strategies to protect personal information

Once your entity has collected and holds personal information, you need to consider what appropriate security measures are required to protect the personal information. This will need to be considered in regards to all of your entity's acts and practices. Part B of this guide sets out examples of key steps and strategies you should consider taking in order to protect the personal information you hold to satisfy your security obligations under the Privacy Act.

[16] See the Own motion investigation report AICmrCN 5. This case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach. Failures at a number of levels aligned to create circumstances that enabled a breach to occur.

[17] This approach is based on the 'Swiss cheese' or 'cumulative act effect' model of accident causation which is an illustration of how organisational failures at a number of levels can combine to create a situation in which human error can trigger a data breach. This is a model used in risk analysis and risk management originally propounded by Dante Orlandella and James T. Reason in 1990.

5. Destroy or de-identify personal information

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[18] This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.

Destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy and is discussed in Part B.

[18] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.

Part A — Circumstances that affect assessment of reasonable steps

What qualifies as reasonable steps to ensure the security of personal information depends on the circumstances, including the following:

- the nature of your entity
- the amount and sensitivity of the personal information held
- the possible adverse consequences for an individual in the case of a breach
- the practical implications of implementing the security measure, including the time and cost involved
- whether a security measure is itself privacy invasive.

These circumstances will also influence the reasonable steps you should take to destroy or de-identify personal information.

The examples of OAIC investigations discussed below are intended to assist an entity to understand our guidance. They reflect a point in time circumstance in relation to the particular organisation.[19] Even slight changes to the facts expressed in the examples may lead to a different result.

Nature of the entity

The size of your entity, its resources, the complexity of its operations and the business model, are all relevant to determining what steps would be reasonable to protect the personal information you hold. For instance, a franchise or a business using outsourcing is likely to provide access to its personal information to third parties (franchisees and contractors). The reasonable steps it takes may be different to those it would take if it did not operate in this manner.

Example 1:

An investigation into a telecommunications company following allegations that customer information had been compromised showed that the company's business model provided access to the company's databases of customer information to dealership employees via a shared store login ID.

Although the use of shared logins and the wide availability of full identity information is an inherent personal information security risk, in this instance the risk was increased by the fact that the entity had less control over information being accessed through dealerships, and no way of tracking or auditing who was accessing the information.

Read the full investigation report for Example 1

[19] The examples of OAIC investigations were undertaken before the commencement of the APPs on 12 March 2014 and therefore refer to the National Privacy Principles (NPPs), specifically NPP 4 (replaced by APP 11). However the examples are still relevant in relation to the circumstances that will affect whether an entity has taken reasonable steps to protect personal information under APP 11.

When you outsource any of your personal information handling to a third party (including to a cloud service provider), and you continue to 'hold' that information, you will still be subject to APP 11. Part B sets out steps to assist you when implementing information handling practices.

Example 2:

The information handling practices of a telecommunications company and its internet service provider (ISP) were considered in an investigation following media reports that a server holding the telecommunications company's customer personal information had been compromised by an external attack.

The investigation found that the telecommunications company and the ISP failed to take reasonable steps to manage and protect personal information held on the compromised server. For example, it was found that the telecommunications company did not have adequate contractual measures in place to protect the personal information held on the compromised server.

Read the full investigation report for Example 2

If you are disclosing to an overseas recipient you may need to take further steps to comply with APP 8, the cross border disclosure principle.[20]

Amount and sensitivity of personal information held

Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it.

The community generally expects that their sensitive information will be given a higher level of protection than non-sensitive information. This expectation is reflected in the increased privacy protections which apply to the handling of sensitive information.

Although it is not defined as sensitive information under the APPs, people often expect that their financial information will be given a high level of protection. The protections in the Privacy Act in relation to credit reporting information and tax file numbers reinforce this.

[20] See APP guidelines, Chapter 8 for further information.

Example 3:

The sensitivity of the information was taken into account in an investigation into a telecommunications company following media allegations that personal information of the company's customers was accessible online, which was confirmed by the company.

The personal information of approximately 15,775 customers was compromised, including full names, addresses and phone numbers, including 1,257 customer accounts with silent numbers. The Commissioner stated that a breach of this type of personal information for the 1,257 customers with silent number was not low risk. Further, the Commissioner noted that different risk levels may require an entity to take different security precautions in order to meet the requirements of the Privacy Act. The Commissioner stated that it was a reasonable step for the company to implement security processes and procedures to address the heightened risk environment.

Read the full investigation report for Example 3

Adverse consequences for an individual

When you are assessing the steps that you will take to protect personal information, you should consider the possible adverse consequences for the individuals concerned if the information is not secured. This may extend to material harm from identity theft or fraud.

The mishandling of some kinds of sensitive information, such as health information that identifies an individual's medical condition, may:

- provide the basis for discrimination or other forms of harm
- lead to humiliation or embarrassment, or undermine an individual's dignity.

The likelihood of harm occurring will be relevant in considering whether it is reasonable to take a particular step.

Example 4:

The necessity of considering the risk of adverse consequences is highlighted by a case where an Australian Government department published statistical data of highly vulnerable people without taking appropriate steps to ensure it was not identifiable.

An investigation found that the department was aware of the privacy risks of embedding personal information in publications, but that their systems and processes failed to adequately address those risks. The likelihood of harm to the individuals affected was a key consideration in assessing whether the department had taken reasonable steps.

Read the full investigation report for Example 4

Practicality of implementation

The practicality of implementing a security measure, including the time and cost involved, will influence the reasonableness of taking that step.

However, you are not excused from taking specific steps to protect information just because it would be inconvenient, time-consuming or costly to do so. Whether these factors make it unreasonable to take particular steps depends on whether the burden is excessive in the specific circumstances.

In deciding whether these factors make a step unreasonable, you should have regard to other circumstances such as the sensitivity of the personal information and the risk to an individual if that information is misused, interfered with, lost, or inappropriately accessed, modified, or disclosed.

Example 5:

An investigation into a medical centre found that there were boxes of unsecured medical records being stored in a garden shed at a site no longer occupied by the medical centre.

The medical centre advised the Commissioner that patient health records were transferred from the locked room inside the former premises to a garden shed at the back of the site (so that renovations for sale of the site could occur). The garden shed door was locked with padlocks.

The Commissioner found that the medical centre did not take reasonable steps to protect the personal information, some of which was also sensitive information. Further, the Commissioner did not consider there to be any circumstances in which it would be reasonable to store health records, or any sensitive information, in a temporary structure such as a garden shed.

Read the full investigation report for Example 5

Privacy invasiveness

It may not be reasonable to implement a security measure if it is itself privacy invasive. For example, requiring users to supply extensive personal information to identify themselves prior to giving access to their records under APP 12 may result in collecting personal information that is unnecessary (contrary to APP 3).[21]

In that instance, you will need to balance what you need to do to prevent disclosure of personal information to the wrong person with the need to ensure that access is given on request.

[21] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

Part B — Steps and strategies which may be reasonable to take

Appropriate security measures for protecting personal information need to be considered in regards to all of your entity's acts and practices. This section outlines examples of key steps and strategies you should consider under the nine broad topics listed below. It includes a number of questions to ask yourself when considering or implementing these steps and strategies.

- Governance, culture and training.
- Internal practices, procedures and systems.
- ICT security.
- Access security.
- Third party providers (including cloud computing).
- Data breaches.
- Physical security.
- Destruction and de-identification.
- Standards.

These steps and strategies are not intended to be prescriptive or exhaustive and it may not be necessary to take all the steps and strategies outlined below. You should also consult relevant standards and guidance on information security including any which are particular to your sector or industry (see 'Standards' and 'Information security resources' below).

The steps and strategies vary in ease of implementation and the impact that they will have on users. What is reasonable in the circumstances may vary between entities, and may change over time, for example, as a result of technological change or if you become aware that security measures that previously protected personal information are no longer adequate.

You should be fully aware of all the personal information you handle, where it is kept and the risks associated with that information before deciding what steps to take. You could undertake robust information asset management by developing and maintaining a list or register which provides a high level description of the types of and location of personal information you handle. This will help ensure that your personal information security measures are comprehensive.

Many of the steps and strategies in this guide may also assist you in protecting other types of information, such as commercially confidential information.

Governance, culture and training

Fostering a privacy and security aware culture

Your privacy and security governance arrangements should include appropriate training, resourcing and management focus to foster a privacy and security aware culture among your staff. Personal information security should be an integrated component of your entire business and not left to the compliance or ICT area alone. The creation of this culture will require the active support of and promotion by, senior management.

Insufficient interest in personal information security from staff, in particular senior management including the board (or equivalent decision making body), can lead to threats to the security of personal information being ignored and not properly attended to. Appropriate training can assist in mitigating these issues and making staff aware of common personal information security threats (see 'Personnel security and training' section below).

If your entity has experienced a significant breach of personal information security, the focus of your senior management should be to look at whether significant cultural changes are needed to improve security in the long term rather than relying on superficial solutions or treating such issues as 'someone else's problem'.

Oversight, accountability and decision-making

You should establish clear procedures for oversight, accountability and lines of authority for decisions regarding personal information security. You could have a body or designated individual/s that are aware of what personal information you hold, where and how it is held and responsible for ensuring that it is held securely. This role could include defining information security measures and implementing and maintaining those measures. This role should be overseen by, and accountable to, your senior management.

- Are privacy and personal information security steps and strategies driven by your senior executives?
- Do the governance arrangements foster a privacy and security aware culture among your staff?
    - Do the governance arrangements promote awareness and compliance with personal information security obligations?
    - What governance arrangements do you have in place?
- Are there clear procedures for oversight, accountability and lines of authority for decisions related to personal information security?
    - Is it clear who is responsible for the overall operational oversight and strategic direction of your information handling projects?
    - Are there distinct areas or persons who have responsibility for security and privacy issues?
        - Are these areas or persons aware of what personal information you hold and where and how it is held?

- If there are several areas or teams responsible for information security and privacy, are there governance arrangements in place to ensure that they work together, creating a focal point for privacy advice and solutions and preventing silos?
- Are regular meetings held at the senior management and operational level to discuss security and privacy issues and incidents?

- Do your change management processes include consideration of the effect of changes on personal information security?
- Do governance arrangements include risk management and business continuity plans?
- Are there ICT governance protocols in place? For example are there persons responsible for the accreditation and approval of personal information security controls to ensure that each control is effective and appropriate?

Personnel security and training

Personal information security includes ensuring your entire staff are aware of their privacy and security obligations (including senior management). Human error can be a contributing cause to data breaches and undermine otherwise robust security practices where the systems have not been designed to deal with it.[22]

It is therefore important that all staff understand the importance of good information handling and security practices. Privacy training may help staff understand their responsibilities and avoid practices that would breach your privacy obligations. Training should take into account new starters, contractors and temporary staff.

- Where appropriate, do staff have appropriate security clearances or undergo security vetting?
- Are staff provided with training on physical and ICT security and the handling of personal information?
  - When is training provided to new starters?
  - Is training also provided to short term staff and contractors?
  - Is refresher training provided to your staff and does this occur on a regular basis?
  - Are your staff informed of your internal practices, procedures and systems which relate to the handling of personal information? (see 'Internal practices, procedures and systems' section below)
  - How are your staff informed of changes to these practices, procedures and systems?
- Is personal information security training of staff considered at the project design stage?

[22] See the Own motion investigation report AICmrCN 5. The case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach.

- Is there an appropriate amount of training, resourcing and active management support to promote a privacy and security aware culture?
  - Does training emphasise to staff the importance of not accessing personal information or databases unnecessarily?
  - Does training make it clear to staff what would constitute misuse of personal information?
  - Does training cover identity authentication procedures?
  - Does training emphasise to staff the importance of authentication processes not infringing customer/client privacy?
  - Does this training cover recognising and avoiding inadvertent disclosures?
    - When verifying an individual's identity?
    - When publishing files online — are staff trained to identify and remove embedded personal information not intended for public release?
- Does training address the need to avoid weak passphrases and passphrase reuse?
- Are staff reminded on a regular basis of their obligations to handle personal information appropriately?
  - Are there signs in the workplace or alerts on computer systems?
  - Do computer logon screens outline staff privacy and security responsibilities?
- When a staff member moves to a different position, or leaves your organisation or agency, is their access to personal information reviewed or revoked?
- Are staff trained to report privacy issues to the area or persons who have responsibility for security and privacy issues?
- Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and 'social engineering'?
- Are staff advised on how to mitigate against unauthorised access if they discuss customers' or clients' personal information over the telephone?
- Are there procedures governing the printing of documents containing personal information?
- Is there a policy that covers information security when staff members work offsite, such as from home, a secondary site office or a temporary office?
  - What standards of physical security are applied to those workspaces, for example, the appropriate storage of physical files?
  - If employees are given remote access to work ICT systems, what measures are in place to secure this access?
  - Who has overall responsibility for the security of personal information at those workspaces?

- Are there clear polices governing the use of end-user mobile devices, including use of staff's own devices (known as 'Bring Your Own Device (BYOD)') and procedures for taking work home?
    - Are there minimum standards for security of end-user mobile devices (such as password protection, encryption)?
    - Are return address labels placed on end-user mobile devices in case of loss?
    - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices, including the risks associated with BYOD practices?
    - If it is necessary for staff to take personal information off the premises, what steps do you take to ensure the security of personal information that is removed?
    - Is confidential business information segregated from personal user information?

Internal practices, procedures and systems

Under APP 1.2, entities are required to take reasonable steps to establish and maintain practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code.[23]

For the purposes of APP 11, you should document the internal practices, procedures and systems that you use to protect personal information. Your documentation should outline the personal information security measures that are established and maintained against the risks and threats to personal information. These documents should be regularly reviewed and updated to ensure they reflect your current acts and practices.

You could also consider documenting the security choices you have made about your security profile, including the reasons why you have or have not adopted specific personal information security measures.

Internal practices, procedures and systems which relate to personal information security may be addressed in a single policy or in a number of separate policies.[24] Additionally, you should make sure that staff are aware of, and have access to, these policies and are trained regarding their responsibilities (see 'Governance, culture and training' section above).

- Do you have policies which address personal information security matters, such as the physical, ICT and access security and other appropriate personal information handling practices?
    - Did a PIA and an information security risk assessment inform the development of these policies?
    - Are your documented policies easy to understand?

[23] For further information see the APP guidelines, Chapter 1.

[24] Use of the term 'policy' in this section refers to your entity's internal documentation regarding its personal information security profile, not its APP privacy policy which is discussed in APP 1.3-1.6.

- If there are multiple policy documents involved, is it clear how they relate to each other, for example their hierarchy or order of importance?
- Do the policies use language and concepts that are consistent with the Privacy Act?
- Do your policies refer to your obligations under the Privacy Act and other laws to protect personal information? Do they clearly explain how these obligations underpin these policies?
- Are all staff, including short-term staff and contractors, aware of and able to access these policies easily?
- Do these policies reflect your current acts or practices? Are mechanisms in place for ensuring that policies are updated and regularly reviewed?
- Are mechanisms in place to enable staff members to seek clarification or suggest updates?
- How do you ensure compliance with internal policies, for example, are there designated privacy officers and regular reporting to the entity's governance body to ensure this occurs?
- What steps do you take if it becomes evident that staff members are not observing elements of your policies?
- Is there a conflict of interest policy in place that instructs staff members on how to proceed if they handle personal information relating to a person known to them?

ICT security

Effective ICT security requires protecting both your hardware and software from misuse, interference, loss, unauthorised access, modification and disclosure. However, ICT security measures should also ensure that the hardware, software and personal information stored on it remain accessible and useful to authorised users.

It is expected that entities regularly monitor the operation and effectiveness of their ICT security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of personal information.

You should be aware of the personal information you hold on your ICT system and where it is located. Your ICT security measures should ensure that all of your systems are secure and that they provide a safe environment for your:

- staff to carry out your business
- customers to interact with your agency or business, for example when they make payments or provide their banking details and/or other personal information.

You need to consider the security of all systems that use or interact with your ICT system. This includes securing your website(s), social media platforms, mobile device applications

(apps)[25] along with Internet connected end-user mobile devices (such as smartphones, tablets and laptops), portable storage devices, desktop terminals, kiosks, as well as Wi-Fi networks, remote access and other aspects of your systems.

ICT security measures help mitigate the risks of internal and external attackers and the damage caused by malicious software such as malware, computer viruses and other harmful programs. These programs can be used to gain unauthorised access to your computer systems in order to disrupt or disable their operation and steal any personal information stored on those systems. ICT security measures can also help mitigate the risks of internal threats.

As well as ICT security against external and internal threats, it is important to consider the possibility of:

- human error (for example, misplacing devices such as laptops and data storage devices, noting that encryption and password protection can mitigate this risk)
- hardware or software malfunctions
- power failure
- system failure caused by natural disasters such as earthquakes, floods, and extreme weather conditions.

Software security

You should consider whether the software you use is sufficiently secure. Errors made during software development can potentially result in privacy breaches.

- Do you regularly review your software security to confirm its continued effectiveness? Is software tested to ensure that there no flaws which can result in privacy breaches?
- Has security software been deployed across all network components (for example on servers and network gateways), not only workstations?
- Are the latest versions of software and applications in use?

Patches can result in a number of extra functions and features that should be assessed for their privacy impacts before they are installed.[26]

- What processes are in place to ensure that patches and security updates to applications and operating systems are installed as they become available?

[25] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services. The OAIC's *Mobile Privacy: A Better Practice Guide for Mobile APP Developers* is available on the OAIC website.

[26] Patches are software that is used to correct a problem with a software program or a computer system.

Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack, and can make it harder for malware to run or an attacker to gain access.

- Are operating system functions that are not required disabled (for example AutoPlay or remote desktop access)?

There is a risk that content delivered through websites can be used to arbitrarily access system users' files or deliver malicious code. This risk can be reduced by ensuring that software applications and web browsers, including 'add-ons' or 'plug-ins' are up to date.[27] Disabling unused applications may also assist in preventing unauthorised access to a computer system.

- Are applications and web browsers configured for maximum security (eg. plug-ins up to date, unused applications disabled)?
- Are add-ons and plug-ins regularly reviewed and updated?

If you are downloading or using web applications (such as web-based email, wikis, directly updating personal details on databases) or importing data to a system, you should ensure that appropriate security and scanning measures are in place.

- Are all email attachments received from an external source scanned before they are opened?
- Are computer files scanned and checked for abnormalities at workstation level?
- Do you have security measures in relation to web applications?

Encryption

Encryption is important in many circumstances to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted copy of your encrypted information.

- What encryption methods do you use? Are they reviewed regularly to ensure they are effective?
- Have you considered whether you should employ encryption of:
    - Databases used to store personal information?
    - Servers?
    - Backups?
    - Information stored in third party cloud servers?
    - Internal network communications, such as email or file shares?

[27] Add-ons and plug-ins are software that add specific functions to a browser

  - End-user mobile devices, such as smartphones, tablets and laptops, including BYOD?
  - Portable storage devices?
  - Data in transit, for example data transferred over the Internet?
- How are decryption keys managed?[28]
- Do you enable encrypted communications on your website (for example, for making payments)?
- Is there another unencrypted copy of your encrypted data?

Network security

You need to have appropriate security controls in place to protect your network. The security controls that are appropriate will depend on the circumstances.

Intrusion prevention and detection systems can be an effective way of identifying and responding to known attack profiles. This may include using firewalls, which control the incoming and outgoing network traffic, and software applications, such as filtering, that monitor network or system activities for malicious activities, anomalous behaviour, or policy violations.

- Do you employ and maintain an intrusion prevention and detection system and regularly analyse event logs?
- What sorts of firewalls are employed and are they appropriately configured?
- Is both incoming and outgoing web traffic filtered?
- How do you monitor and detect unauthorised downloading, transferring or theft of bulk data, for example through the use of personal storage devices?

Spammers may use spoofed email to try to bypass filters and make it appear as though email comes from a legitimate source.[29] Such emails may ask the recipient to provide their own or other individuals' personal information.

- Do you have systems in place to protect your email systems from malware, spam and spoofing, including blocking spoofed email?
- Do you employ email validation and authentication systems, for example the Sender Policy Framework[30] and Domain Keys?[31]

[28] Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to easily recover the contents of encrypted information, the correct decryption key is required.

[29] Spoofed email is email in which parts of the email header are altered so that it appears to have come from a different source.

[30] Sender Policy Framework is an email validation system designed to detect email spoofing by allowing receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorised by that domain's administrators.

[31] DomainKeys is an email authentication system designed to verify the domain of an email sender and that the email message was not modified in transit.

Separating an entity's network into multiple functional segments makes it difficult for an intruder to propagate inside the network. Proper network segmentation assists in the creation and maintenance of network access control lists. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.

- Is the network segmented and segregated into security zones?
- Are different security measures applied to different security zones, depending on the type of information in that zone and the risks associated with it?
- Does the information with the highest risk have the highest level of protection applied?
- What steps have been taken to ensure that this information is not inadvertently taken outside of the secured environment?
- Are downloaded files quarantined from the network until it is established that they are safe (opened in a segregated testing environment such as a sandbox)?

Whitelisting and blacklisting

Whitelisting and blacklisting are ways of controlling the content, applications or entities that are allowed to run on or access a device or network.[32]

Both can prevent potentially harmful material from accessing your system. Whitelisting may offer greater protection than blacklisting as it is not dependent on identifying the material to be blocked. However, a drawback is that it can also block harmless content that is not whitelisted. Reputation-based lists used for blacklisting need to be maintained and updated to be effective due to the rapid pace with which malicious sites come and go.

- Is whitelisting of applications, email attachments and web domains and IP addresses employed?
- If not, has blacklisting of applications, email attachments and web domains and IP addresses been used instead?
    - If so, what steps are in place to ensure the blacklist remains relevant, up to date and complete? For example, is the blacklist automatically updated from time to time?

Testing

Testing of ICT systems should occur during their development, transition to operations and regularly once they are operational. Depending on the situation, you may wish to consider penetration (or vulnerability) testing to discover security weaknesses, or configuration reviews, to test whether networks are operating towards a certain standard.

[32] Whitelisting is permissive — it is a list of the content, applications or entities that are allowed. Blacklisting is prohibitive — it is a list of the content, applications or entities that are not allowed.

You need to consider how to scope your testing — remember that testing only discrete elements of your ICT system may miss systemic issues.

- How often is testing conducted?
- Does it cover all aspects of the system?
- Who is responsible for conducting testing (eg. internal, independent)?
- How is test data handled?
- Is actual personal information or dummy data used for testing? If actual personal information is used:
  - has a PIA and information security risk assessment been undertaken to assess the personal information flows caused by the testing?[33]
  - do your internal practices, procedures and systems reflect the use of personal information for testing?
- If testing identifies weaknesses, how is this reported and addressed?

Backing up

To prevent personal information you hold from being lost, you should make copies of important files and store them on a physical device or online using a cloud-based storage solution.

- Are backups set up to run frequently?
- Is all essential information included in backups?
- How far back is data recoverable?
- Do you have a data retention policy which reflects APP 11.2?
- Do you review your backups to check that personal information that is no longer needed is:
  - destroyed or de-identified
  - if contained in a Commonwealth record, handled in accordance with the Archives Act
  - if required by law or a court/tribunal, is retained? (see 'Destruction or de-identification of personal information' section below)
- Are backups regularly tested to see if the data is recoverable?
- Are physical devices used to store your backup files kept in a secure location?

[33] An example of a 'use' that an individual may be taken to reasonably expect is use for the secondary purpose of a normal internal business practice, such as auditing, business planning, billing or de-identifying personal information. The OAIC generally considers that the use of personal information to test ICT security systems may be a normal internal business practice in limited circumstances, such as where it is unreasonable or impracticable to use de-identified or dummy data (subject to the exception in APP 6.2(a)). For further information see APP guidelines, Chapter 6, paragraph 6.22.

- Are backups stored remotely to protect from natural disasters?

Email security

Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email.

- Do you avoid sending certain types of personal information via unsecured email (for example sensitive information)?
- Do you use secure methods for communicating information, such as a secure website or to a secure online mailbox?
- Do you use secure messaging where appropriate and available?
- Do you obtain a recipient's consent to send their own personal information to them via email?
- Do you validate the email address with the recipient before sending the unencrypted email to reduce the chance of unauthorised disclosure to a party who is not the intended recipient?
- Do you ensure that accurate records are kept regarding when external emails are sent and received?
- Do you only send sensitive information or large amounts of non-sensitive personal information by email as an encrypted or password protected attachment?

Access security

Access security and monitoring controls help you protect against internal and external risks by ensuring that personal information is only accessed by authorised persons.

'Unauthorised access' is a separate concept from 'disclosure', as an entity is not taken to have disclosed personal information under APP 6 (Use and disclosure) where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, the entity may breach its security obligations under APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access.

Trusted insider risk

You need to guard against internal threats such as unauthorised access or misuse of personal information by your staff, including contractors (the trusted insider risk). Trusted insider breaches can occur when staff mishandle personal information while carrying out their normal duties. These actions are often motivated by personal advantage, for example insiders accessing personal information for financial gain.

To minimise this risk you should, when possible, limit internal access to personal information to those who require access to do their job (ie provide access on a 'need to know' basis). Limiting such access is an important personal information security mechanism.

If someone is transacting with you using a pseudonym, you could also consider further restricting access to personal information that is linked to that person to protect the pseudonym.[34]

- Do you limit access to personal information to those staff necessary to enable your entity to carry out its functions and activities?
- Is the number of users with administrative privileges limited to staff requiring those privileges?
- Is access revoked promptly when no longer required?
- Have you considered restricting access to personal information when a customer/client is using a pseudonym?
- Have you considered physically disabling USB or other external port access to devices or disabling internal cd/dvd writers in devices?
- Have you considered employing remote wiping software to allow for the deletion of personal information stored on end-user devices which have been lost or stolen?

Identity management and authentication

You should have processes in place to identify individuals accessing your systems and control their access by associating user rights and restrictions with their identity. This will ensure that only authorised persons can access your systems.

Authentication is a key part of this process and is often managed by providing one of three factors— something one knows (such as a password or code), something one has (a physical token, such as a bank card, security pass, or a mobile phone to receive SMS confirmation), or something one is (biometric information such as a fingerprint). 'Multi-factor authentication' requires at least two factors.

Appropriate authentication can be used to limit a person's access both to the system or network and also to the information contained within it. It can also assist in mitigating security risks such as 'social engineering'[35] (including 'phishing' and 'spear phishing'[36]).[37]

- What factors do you use for authentication?
- Is multi-factor authentication employed in circumstances that may pose a higher security risk (such as remotely accessing a system or where they are accessing sensitive/restricted personal information)?

[34] APP 2 covers issues related to anonymity and pseudonymity.

[35] 'Social engineering' is a term used to describe manipulating individuals into revealing confidential information or performing actions such as granting access to systems.

[36] 'Phishing' typically involves sending an email that appears to come from a legitimate organisation and attempts to trick the recipient into supplying personal information. 'Spear phishing' is a personalised attack utilising personally relevant information to attempt to appear legitimate to a particular user.

[37] According to Verizon's *2014 Data Breach Investigations Report*, p.10 phishing was the third most commonly seen threat action in 2013, see www.verizonenterprise.com/DBIR/2014/.

- Have technical solutions which block or mitigate the effects of phishing, spear-phishing and social-engineering attacks been applied (where appropriate)?

Access to non-public content on web servers

If you host content that is not intended for public release (non-public content) on your web servers, you should consider storing this content elsewhere or restrict access to this information to authorised and authenticated users only. This ensures that non-public content will not be accessed by unauthorised third parties, including search robots[38] such as GoogleBot.[39] In conjunction with authentication, you should also disable directory browsing when configuring web servers.[40]

- Are there clear policies and procedures in place governing the identification and removal of embedded personal information from files before they are published online where the information is not intended for public release?

If you store non-public content on your web servers:

- Do you have access controls in place?
- Can the information be stored on a separate system which is not publicly accessible?
- Have you disabled directory browsing on your web servers?
- Are web servers configured to request search robots such as GoogleBot (via the robots.txt.file)[41] not to index, archive or cache files containing personal information?
- Do you regularly review and monitor your web servers to ensure that:
    - files containing non-public content are not vulnerable to being accessed by unauthorised persons?
    - you are aware of unusual or anomalous traffic on the website? (see 'Audit logs, audit trails and monitoring access' section below).

[38] Search robots or bots are software programs which run automated repetitive tasks over the Internet. They are most commonly used by web search engines and other sites for 'Web crawling' or 'Web spidering'. This involves a search engine using bots to discover new and updated pages which are then added to the search engine's index of Web content.

[39] GoogleBot is Google's web crawling bot.

[40] Directory browsing gives permission to users to view a listing of the files in a web server. If directory browsing is disabled, an 'Access Forbidden' error message is displayed if the user attempts to access either a file or folder on the web server.

[41] One way to prevent GoogleBot from crawling content on a website is to use robots.txt to block access to files and directories on a server. 'Robots.txt' is a protocol used to request cooperating search robots not to access all or part of a website which is otherwise publicly accessible. Search engines comply with 'robots.txt' voluntarily and the OAIC has noted that most search engines comply with 'robots.txt', including Google, Bing and Yahoo.

Passwords and passphrases

Your entity should use passwords and passphrases to identify that users requesting access to your systems are authorised users. Passwords and passphrases should be complex enough so that others are not able to guess it, for example using a combination letters, numbers and symbols rather than actual words or common numbers.

- Is password or passphrase complexity enforced? For example, including uppercase characters, lowercase characters, punctuation, symbols, and/or numbers.
  - Are there mechanisms for changing them regularly?
  - Is reuse of passwords or passphrases blocked?
  - Is there a minimum length requirement? Is sharing of passwords or passphrases forbidden?
  - Are passwords or passphrases stored securely, such as in a 'hashed', 'salted'[42] or 'encrypted' format?
- Do accounts lock the user out after a specified number of failed logins?
  - Is a system administrator required to unlock accounts?
  - Do you suspend accounts that are unused or inactive for a period of time?
  - How quickly are accounts removed or suspended once someone leaves the entity?
- Are screen lock programs activated when computers are not in use? Do the screensavers properly blank out computer screens or fill them with moving images or patterns so that no personal information can be displayed when computers are not in use?
  - Do computers automatically lock if left inactive or unattended for periods of time?
  - Are users advised to lock their computers when they leave their desks, even for short periods?
- Are staff (including contractors) trained in the importance of strong passwords or passphrases and how to choose them?

Sometimes passwords are created using patterns that are known only to an entity and its staff (or part of its staff). Whilst each password is unique, there is a risk that a password may be inferred by someone who is aware of the pattern but is not authorised to access the file.

[42] 'Salting' is basically where an additional string of data, such as random numbers or text, is added to the password to make it less predictable and harder to attack, and 'hashing' is where passwords are processed through cryptographic algorithms that convert them into seemingly random characters. While passwords may be guessed through computational 'brute-force' attacks, this becomes very difficult when strong hash algorithms and passwords are used. Hashed passwords are therefore more secure to store than their clear-text passwords. The Australian Signals Directorate Information Security Manual (Control 1252, page 173) requires agencies to ensure usernames and passwords hashed with a strong hashing algorithm and uniquely salted.

Longer password patterns with many variations that are selected randomly rather than following a recognisable or known pattern are less likely to be guessed by unauthorised persons.

- Are passwords generated by patterns which are randomly selected and complex in terms of their length, character and order?

Collaboration

If you collaborate and share personal information with other entities while working on projects, you may continue to 'hold' personal information that is being used by the other collaborator. In these circumstances you must take reasonable steps to protect the information from unauthorised access while in their physical possession, including having effective controls in place to ensure that it is only accessed by authorised persons.

- How is the sharing of personal information managed to ensure access only by authorised persons?
  - How is access monitored?
  - Is the personal information shared using a secure method?
  - Is a platform that is managed, controlled or owned by another entity (such as a contract service provider), used to share the information? If so, what controls are in place to limit access?
  - Is the information encrypted and password protected? How are passwords managed and distributed to the user group?
  - Is there an access control policy in place which applies to everyone handling the personal information?
  - Are there policies and controls in place to prevent the unauthorised downloading, transferring or theft of bulk data shared with other entities, for example through the use of personal storage devices?

Audit logs, audit trails and monitoring access

Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.

Audit trails are used to reconstruct and examine a sequence of activities on a system that lead to a specific event, such as a privacy incident.[43]

Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information.

[43] 'Audit log' and 'audit trail' are defined in the *Australian Signals Directorate Information Security Manual*, Glossary of Terms, p. 308

- What methods do you use to identify inappropriate access of files or databases containing personal information
  - Do you use audit logs and audit trails?
  - Is access by both internal and external persons monitored? Is there a method for identifying anomalous behaviour?
  - Are these measures mainly reactive (review of logs, responding to incidents) or do they also involve real time or close to real time monitoring of access activity? (also see 'Network security' section above).
- What points of access (such as access to devices, files, networks, databases, and websites) do you audit?
- Are audit logs reviewed on an on-going basis?
  - do you check/audit the activity of administrators?
- Does the audit log or audit trail indicate when an individual has:
  - accessed or viewed material
  - changed or destroyed material, or
  - unsuccessfully tried to access personal information?
- Does the audit log or audit trail enable actions to be linked to individuals, including both regular users and administrators?
- What procedures exist to address any issues, such as anomalous patterns of access, identified during a review of an audit log?
- How long are the audit logs kept for?
  - Are they part of a backup process?
- How are audit logs protected from tampering?
- Do logs or reports contain personal information and if so is it adequately protected?

Individuals accessing and correcting their own personal information

Under the Privacy Act, entities must, on request, give individuals access to the personal information held about them unless an exception applies.[44] Individuals are also able to request correction of the personal information held about them.[45]

- What processes do you have in place to assess requests from individuals to access or correct their personal information?

[44] See APP 12. Along with the right to request access under the Privacy Act, individuals have a right under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to information held by Australian Government agencies.

[45] See APP 13 - where an individual requests an APP entity to correct their personal information, APP 13.1 provides that the entity must take reasonable steps to correct the personal information it holds, to ensure it is accurate, up-to-date, complete, relevant, and not misleading, having regard to the purpose for which it is held'. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

- How do your staff identify customers/clients prior to disclosing their personal information online, by phone or in person?
- What measures do you take to ensure that these authentication processes do not result in collecting personal information that it is not reasonably necessary to collect?

Third party providers (including cloud computing)

Entities that outsource part or all of their personal information handling will need to consider whether they still 'hold' that personal information. If so, APP 11 will apply and you will need to take reasonable steps to comply with APP 11.

General issues

Relevant factors in deciding the steps that are reasonable in the circumstances include whether the third party is subject to the Privacy Act in its own right. Even if the third party is subject to the Privacy Act, if you hold the personal information, you still need to consider what steps are reasonable to protect the personal information. Steps may include influencing the third party's conduct.

Have you:

- conducted appropriate due diligence on the services to be provided (particularly data storage services)?
- considered the scope of the personal information handling services to be provided (for example, will the provider also backup your personal information holdings and if so what data will be captured)?
- considered what security controls and personal information handling measures you expect the third party supplier to use?
- included terms in the contract to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements
- for agencies, complied with s 95B of the Privacy Act which requires agencies to take contractual measures to ensure that a contracted service provider (as defined in the Privacy Act) does not do an act, or engage in a practice, that would breach an APP.[46]

[46] In particular, the agency must ensure that the contract does not authorise a contractor to do or engage in such an act or practice. An agency must also ensure the contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.

Cloud computing

Cloud computing can range from data storage to the use of software programs, with data being stored and processed by the cloud service provider.[47] For instance, an entity can store data on remote servers operated by the cloud service provider rather than storing it on their own servers.

If you continue to 'hold' personal information when storing or using it in the cloud, reasonable steps may include robust management of the third party storing or handling your clients' personal information, including effective contractual clauses, verifying security claims of cloud service providers through inspections, and regular reporting and monitoring.

If you chose to adopt cloud computing you need to assess the security controls of the provider to ensure that you continue to comply with APP 11. However, other APPs may also apply in these circumstances, including APP 8 (where personal information is disclosed to an overseas recipient),[48] and APPs 12 and 13 (access and correction). These are discussed in more detail in the APP guidelines.

You should also consider whether your cloud service provider should be required to have similar controls to those you might apply to your own systems, such as governance arrangements and controls relating to software security, access security and network security set out in the sections above.

- Does the contract require the cloud service provider to put in place reasonable security steps that enable you to comply with your obligations under the APPs?
- From a security controls perspective, do you understand what controls you are responsible for and what your cloud service provider is responsible for?
- Are you able to verify the security controls of the cloud service provider to a sufficient level of detail, such as through independent testing and validation?
- Will those contractual obligations be reasonably easy to enforce from a costs and practicality perspective?
- Is the cloud service provider's information handling practices certified against information security standards (such as the ISO 27000 group)?[49]

[47] Cloud computing services have been defined as a way of sourcing and delivering ICT which enables convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications and services). The Australian Government has adopted the US Government's National Institute of Standards and Technology definition for cloud computing. For further information see the Australian Government's Cloud Computing Policy and supporting material which apply to the use of cloud services by Commonwealth entities, available on the Department of Finance's website at www.finance.gov.au/cloud/.

[48] You may also need to consider the data protection or privacy legislation in place where the data is stored by the cloud provider, as well as any other jurisdictions the cloud service provider may be subject to.

[49] In 2014, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) also published ISO/IEC 27018:2014 which relates to the implementation of measures to protect personal information while it is being processed in the public cloud. The standard uses a definition of 'Personally Identifiable Information' adopted from ISO/IEC 29100:2011. If adopting this standard, entities

- Is the cloud service provider required to notify clients in the event of a data breach and does it have reasonable data breach response processes? In particular, are sufficient controls in place to properly investigate and respond to any suspected or actual breach to determine when and how it occurred, and what was taken?
- Does the cloud service provider enable secure transactions and encrypted storage?
- Have you considered encrypting the data yourself before transmission (rather than relying on the cloud service provider's encryption)?
- Have you considered who is able to decrypt data stored in the cloud?
- Does the cloud service provider intend to use your data for its own commercial purposes (separately or combined with other customers' data)? If so have you considered the security implications, including:
  - can you control the use of your data?
  - is the personal information de-identified before the provider uses it?
  - can you verify that the de-identified personal information cannot be re-identified?
- Does your cloud service provider subcontract to or use the resources of other parties to perform its services, and if so, how do they protect your data?
- Will your data be stored separately from the data of other customers of the cloud service provider; for example, on separate servers?
- Does the cloud service provider possess appropriate data recovery plans to deal with a natural disaster or system failure and prevent disclosure of your information?
- Is your data stored in a format you will be able to access or use if you need to retrieve it or amend it?
- Can the cloud service provider confirm whether it copies or otherwise replicates your information for its internal operational purposes (for example, if it moves your information between its IT assets), and what controls it has in place?
- Can the provider confirm that your information and any copies (including backups) have been destroyed at the conclusion of the contract? Can you retrieve the information?
- How easily can you contact a representative of the cloud service provider with privacy concerns?

must ensure that they apply the definitions of personal information and sensitive information in the Privacy Act. More information can be found in the 'Standards' section below.

Data breaches

In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist you to contain the breach and manage your response. Ensuring that staff (including contractors) are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective. The OAIC has published *Data breach notification: a guide to handling personal information security breaches*.

- Is there a data breach response plan and does it flow logically from any broader information security plan?
  - Is the plan regularly tested?
  - Does the plan include a strategy to assess and contain breaches?
  - Does the plan clearly identify those actions that are legislative or contractual requirements?
  - Are your staff educated about the plan and how to identify and respond to data breaches?
  - Does the plan enable staff to identify data breaches and require that breaches be reported?
  - Does the plan establish clear lines of command and indicate responsible officers?
  - Does the plan outline clearly when affected individuals should be notified of breaches?
  - Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?
- Are you required to notify affected individuals and the OAIC under law?[50]

Physical security

Physical security is an important part of ensuring that personal information is not inappropriately accessed. You need to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, you should consider whether the workspace itself is designed to facilitate good privacy practices.

- What measures are used to control access to the workplace?
  - Are security and alarm systems used to control entry to the workplace?
  - Is it possible to identify staff movements from access logs?
- Are work areas with particular access to personal information (for example, human resources sections, complaints handling sections) physically segregated from other areas of business?

[50] Particular entities have mandatory data breach notification reporting obligations under s 75 of the PCEHR Act.

- Is there a record management system that identifies files and the location of responsible staff that contain personal information?
- Have privacy and security been considered when designing the workspace?
  - Are workstations positioned so that computer screens cannot be easily read by unauthorised third parties?
  - Do visitors have access to general workspaces or are there designated areas for them?
  - Are employees working on sensitive matters able to do so in a private/secure space, particularly in open plan workplaces?
  - Do employees have access to secure storage spaces near their workstations to secure documents temporarily?
- Is there a clean desk policy where personal information is being handled? Is it enforced?
- What provisions are made for securing physical files containing personal information?
  - How is the movement of physical files recorded?
  - Are storage and movement of files containing personal information audited or monitored?
  - On what basis is access to physical files granted?
  - If files are placed in lockable cabinets or similar, are these storage units kept locked? How is access to keys controlled?
- Are there procedures governing the transmission or transport of personal information to offsite work locations?

Destruction or de-identification of personal information

Where an entity holds personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information (APP 11.2) — in some cases, one or the other may be more appropriate. This obligation applies even where the entity does not physically possess the personal information, but has the right or power to deal with it.[51]

However, depending on the type of entity and the type of personal information involved, you may have specific obligations under law or a court/tribunal order to retain and/or destroy or de-identify personal information. Agencies also have specific retention obligations for personal information that forms part of a Commonwealth record.

- Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained under law or a court/tribunal order, destroyed or de-identified?

[51] See Chapter 11 of the APP guidelines for further guidance on the destruction or de-identification of personal information.

- Are your staff informed of document destruction procedures?

Destroying personal information — irretrievable destruction

Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an entity to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

- Are your staff informed of document destruction procedures?
- Is destruction of personal information done in-house or outsourced?
    - If outsourced, what steps have you taken to ensure appropriate handling of the personal information?
- Has personal information contained in hard copy records that are disposed of through garbage or recycling collection been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding?
- Is hardware containing personal information in electronic form properly 'sanitised' to completely remove the stored personal information?
- Have steps been taken to verify the irretrievable destruction of personal stored by a third party on a third party's hardware, such as cloud storage, where the third party has been instructed by the organisation to irretrievably destroy the personal information, have steps been taken to verify that this has occurred?
- Are back-ups of personal information also destroyed? Are backups arranged in such a way that destruction of backups is possible? If not:
    - have steps been taken to rectify this issue in the future
    - has the backed-up personal information been put beyond use?
- How is compliance with data destruction procedures monitored and enforced?

Destroying personal information held in electronic form — putting beyond use

Where it is not possible for an entity to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'. For example, this could include where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information.

Personal information is 'beyond use' if you:

- are not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surround the personal information with appropriate technical, physical and organisational security. This should include, at a minimum, access controls including logs and audit trails, and
- commit to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format.

- Where it is not possible to irretrievably destroy personal information held in electronic format has the organisation taken steps to put the information 'beyond use'?

De-identifying personal information

De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the entity or a third party, but you should consider whether de-identification is appropriate in the circumstances.

Personal information is de-identified under s 6 of the Privacy Act, 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

- Do you have policies, practices and procedures in place to determine when it is appropriate to de-identify personal information?
  - How do you manage and mitigate the risk of re-identification?
  - Have steps been taken to verify the de-identification of personal stored by a third party (such as cloud storage)?

Standards

'Standards' are documents that set out requirements, specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform in the way they are intended.[52] Standards can include guidelines, handbooks, manuals or policies and may be general or specific to particular industries or sectors, or practices.

Entities should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to their sector or industry (for example the *National eHealth Security and Access Framework*, which is relevant to the health sector).

Australian Government agencies must apply the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government. They may also be used by other government agencies (including state and territory agencies) and the private sector as a model for better security practice.

[52] The term 'standards' is defined on the Standards Australia website at www.standards.org.au.

You may also want to consult the ISO/IEC 27000 series of information security management standards and the ISO/IEC 31000 of risk management standards published by both the International Organization for Standardization and the International Electrotechnical Commission, parts of which have been adopted by Standards Australia.[53] The 27000 series of standards provide recommendations on information security management, risks and controls. The 31000 series relates to standards for the design, implementation and maintenance of risk management processes. Compliance with standards can be tested internally or certified by a third party.

Adopting a standard is one way that you can gain some confidence regarding your security practices, but complying with a standard does not of itself mean that you have taken reasonable steps to protect personal information. It may be a reasonable step, but you may also need to take further action to meet your obligations under APP 11.

You may also seek to use certification of compliance with a standard as an assurance that you are protecting personal information. However, you will need to be aware of the scope of any certification, for example, whether it includes an assessment of the implementation of the relevant standard/s in practice; or the suitability of the risk profile underpinning the adoption of the standard/s. You will also need to aware of the extent to which you may rely on any certification of your processes or the processes of a party you are dealing with. Relying on the certification of your processes or the processes of a party you are dealing with may not of itself be considered 'reasonable steps' for the purposes of APP 11. You may need to take further action to meet your security obligations under APP 11.

In adopting any standard, you must make sure that you apply the definition of personal information and sensitive information from the Privacy Act, and not any other similar definitions that might by imported by or used in the standard.

- Have you considered standards particular to your industry or sector?
- If you have decided not to adopt a widely used standard, are the reasons for this decision clearly documented?
- Do you ensure that the standards you employ are the most current and appropriate?
- Is internal or external auditing undertaken to ensure compliance with relevant standards?
- If you have sought a certification of compliance with a relevant standard, did the scope of the certification include implementation; and the suitability of the risk profile underpinning the adoption of the standard?
- If auditing reveals areas of weakness or non-compliance with a standard, are these reported and addressed in a timely and complete manner?

[53] Further information regarding Australian and international standards is available from the Standards Australia website at www.standards.org.au and the International Organization for Standardization website at: www.iso.org.

Appendix A — Glossary of terms

Unless otherwise stated, terms used in this guide have the same meaning as in the Privacy Act. Some of these terms are explained in more detail in the APP guidelines.

Agency has the meaning set out in s 6(1) of the Privacy Act and includes a Commonwealth Minister, certain Australian Government agencies and the Norfolk Island administration.

APP entity means an agency or organisation and has the meaning set out in s 6(1) of the Privacy Act.

APPs means the Australian Privacy Principles which are set out in Schedule 1 of the Privacy Act.

CII means Commissioner initiated investigation, made under s 40(2) of the Privacy Act, where the Commissioner may, on his or her own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1. Investigations relating to acts or practices prior to 12 March 2014 use the term 'own motion investigation'.

Commonwealth record is defined in s 6(1) of the Privacy Act to have the same meaning as in s 3 of the *Archives Act 1983* (Cth).

CRB means credit reporting body and has the meaning set out in s 6 of the Privacy Act.

Credit provider has the meaning set out in s 6(1) of the Privacy Act.

CR Code means the *registered Privacy (Credit Reporting) Code 2014*, a mandatory code that binds credit providers and CRBs. The CR code supplements the provisions contained in Part IIIA of the Privacy Act and the *Privacy Regulation 2013*. A breach of the CR code is a breach of the Privacy Act.

Cth means Commonwealth.

Data breach means, for the purpose of this guide, when personal information held by an entity is lost or subjected to unauthorised access, use, interference, modification, disclosure, or other misuse.

Discloses is not defined in the Privacy Act and its meaning is discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.57-B.63.

Entity means an agency, organisation or other person covered by the Privacy Act, including those covered by the APPs, Part IIIA and the *Tax File Number Guidelines 2011*.

Holds has the same meaning set out in s 6(1) of the Privacy Act (discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.73-B.76) and as summarised on page 4 of this guide.

Information security means all measures used to protect any information generated by an entity or individual that is not intended to be made publicly available from compromise, loss of integrity or unavailability.

NPPs means the National Privacy Principles, which used to apply to organisations unless an exemption applied. The NPPs were replaced by the APPs on 12 March 2014.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act and, in general, includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers regardless of turnover and a range of small businesses (see ss 6D and 6E of the Privacy Act).

Personal information has the meaning as set out in s 6(1) of the Privacy Act:

'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

Personal information security means keeping personal information secure from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

PIA means privacy impact assessment and is discussed in the OAIC's Guide to undertaking privacy impact assessments.

Privacy Act means the *Privacy Act 1988* (Cth).

Sensitive information has the meaning as set out in s 6(1) of the Privacy Act and includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal record, health information and some aspects of genetic and biometric information.

TFN means a tax file number and has the meaning set out in Part VA of the *Income Tax Assessment Act 1936* (Cth).

TFN information means information that connects a TFN with the identity of a particular individual (for example, a database record that links a person's name and date of birth with the person's TFN).

Uses is not defined in the Privacy Act and its meaning is discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.136-B.138.

Appendix B — Additional resources

OAIC resources

- The *Australian Privacy Principles guidelines*, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.
- The *Privacy Regulatory Action Policy*, which explains the OAIC's overall approach and priorities when using its privacy regulatory powers and making related public communications.
- *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* outlining how the OAIC will approach enforcement issues under the PCEHR Act.
- *Guide to undertaking privacy impact assessments* which provides assistance to entities on designing, conducting and acting on a privacy impact assessment.
- *Data breach notification: A guide to handling personal information security breaches*, which outlines steps that entities should consider in preparing for and responding to information security breaches, including notifying affected individuals.
- *Information Policy Agency Resource 1 — De-identification of Data and Information*, which provides general advice about de-identification, to assist agencies in balancing those objectives in information management.
- *Mobile Privacy: A Better Practice Guide for Mobile APP Developers*, which helps mobile device application (app) developers embed better privacy practices in their products and services, and help developers that are operating in the Australian market to comply with Australian privacy law and best practice.
- *Privacy Business Resource 4 — De-identification of data and Information*, which provides general advice about de-identification, to assist businesses and other organisations to protect privacy when using or sharing information assets containing personal information.
- *Privacy fact sheet 6 — The binding Tax File Number Guidelines 2011 and the protection of tax file number information* — which provides guidance related to the handling of TFNs, including the security obligations of TFN recipients.

Other resources

In addition, the following information security resources may be relevant to entities:

- CERT Australia is Australia's national computer emergency response team. CERT Australia is the single point of referral for cyber security incidents impacting upon Australian networks. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

- *Control Objectives for Information and Related Technology* (COBIT) — COBIT 5 is the latest edition of ISACA's international framework for information technology (IT) management and IT governance.
- International standards published by the International Organization for Standardization (ISO) and Australian standards published by Standards Australia (see also the 'Standards' section in Part D of this guide), including the AS/NZS ISO/IEC 27000 series of information security management standards.
- *OECD Guidelines for the security of information systems and networks* is a framework of principles applicable to the security of information systems.
- The *National eHealth Security and Access Framework* (NESAF) is a comprehensive suite of documents regarding health security for the health industry and specific Australian health organisations. The NESAF aims to assist health organisations in meeting their security obligations.
- *StaySmartOnline* — this website provides guidance to businesses (and individuals) on measures they can take to protect personal and financial information online.
- *Managing the insider threat to your business - a personnel security handbook* - this handbook addresses the risk of the trusted insiders.

The following resources are particularly relevant to Australian Government agencies but are also useful for other organisations and government agencies:

- The *Australian Government Protective Security Policy Framework* (PSPF), which aims to enhance a stronger security culture and provide a common approach to the implementation of protective security by Australian Government agencies and which agency heads are required to apply. The PSPF may also be used by other government agencies (including state and territory agencies) as well as the private sector as a model for better security practice.
- *Information Security Management Guidelines — Risk management of outsourced ICT arrangements (including Cloud)* — the guidelines provide a consistent and structured approach to undertaking a risk assessment when considering outsourced ICT arrangements for Australian Government information.
- *Agency cyber security responsibilities when transacting online with the public* — which aims to assist agencies to understand and address their responsibility to minimise the risk of harm to the public when transacting online with the Australian Government.

- The Australian Signals Directorate (ASD) has a number of ICT security publications. including:
  - *Australian Government Information Security Manual*, which governs the security of government ICT systems
  - *Strategies to Mitigate Targeted Cyber Intrusions* a useful guide for both Government agencies and the private sector that contains a list of strategies to mitigate targeted cyber intrusions.
- The *National Identity Security Strategy* includes standards, best practices resources and tools (such as the Document Verification Service) to help agencies and other types of entities strengthen identification processes, secure identity records and documents and detect identity fraud. Resources are also available under the Strategy to help Australians protect their identity and respond to identity crime.
- The *National e-Authentication Framework*, developed by the Australian Department of Finance, assists Australian Government agencies and state jurisdictions in authenticating the identity of another party to a desired level of assurance or confidence.
- The Australian Government's policy on cloud computing for non-corporate agencies and supporting material on the Department of Finance's website.

HPOS Terms and Conditions of Use and Access.

Australian Government
Department of Human Services

HPOS Terms and Conditions of Use and Access

These Terms and Conditions of Use and Access (Terms and Conditions) apply to all access and use of the HPOS.

on this page

1. About these Terms and Conditions
2. Changes to Terms and Conditions
3. Compliance
4. Accuracy of information and representations and false or misleading information
5. Terms of use of the System
6. Personal Information
7. Security
8. Notification to us
9. Accessibility
10. Changes to the System
11. Subscriptions and email notifications
12. Liability
13. Restriction, suspension and termination
14. Jurisdiction
15. Contra Proferentem
16. Contact Information
17. Declaration
18. Definitions and interpretation
19. AIR Terms and Conditions
20. Department of Veterans' Affairs (DVA) Terms and Conditions

1. About these Terms and Conditions

1. In these Terms and Conditions:
   a. "**you**" or "**your**" is a reference to the user agreeing to these Terms and Conditions and all parties acting on the user's behalf (**agents**);
   b. "**we**", "**our**" or "**us**" is a reference to:
      i. Human Services;
      ii. the Service Supplier; and/or
      iii. the System Operator,
   c. as the context requires; and
   d. "**Terms and Conditions**":

i. means these terms and conditions set out in **clauses 1** to **18**, as amended from time to time in accordance with **clause 2**; and

ii. where **clause 19** applies, includes the AIR Terms and Conditions

2. These Terms and Conditions apply to all access and use of the System using a Digital Credential and apply between:
   a. Chief Executive Medicare and us; and
   b. you and any legal entity that you represent in accessing and using the System and any delegate of yours
3. In using and accessing the System and agreeing to these Terms and Conditions, you warrant that you have the authority of any legal entity you represent to use the System on their behalf and to bind them to these Terms and Conditions
4. These Terms and Conditions constitute the entire agreement between you and us in connection with the System
5. We agree to make the System available to you in accordance with these Terms and Conditions
6. Please read these Terms and Conditions carefully. You agree:
   a. to be bound by these Terms and Conditions every time you use the System, whether you access the System through these Terms and Conditions and by clicking "I agree" or whether you access the System through other web pages; and
   b. that you are responsible for the appointment and management of your delegates and of their use of the System

2. Changes to Terms and Conditions

1. You agree:
   a. that we may change or add to these Terms and Conditions at any time, by giving you notice, which may be provided electronically;
   b. that a message sent to your email address (as held in our records) or by notice published on our Health professionals website is one way of giving you notice electronically;
   c. that if you do not agree to the amendments, you (as your sole remedy) should cease to use the System;
   d. that if you access or use the System after you have been notified of a change or addition to these Terms and Conditions, you will be taken to have agreed to that change or addition in respect of all access to and use of the System after that date; and
   e. that these Terms and Conditions may not be changed orally or by conduct by any person

3. Compliance

1. You agree:
   a. to comply with these Terms and Conditions in relation to your access to, and use of, the System;
   b. that you must ensure that your agents do not do anything that these Terms and Conditions prevent you from doing; and
   c. to inform your delegate(s) and any legal entity that you represent, of these Terms and Conditions and its responsibilities under these Terms and Conditions when using the System
2. You must not assign or sub-licence any rights or novate your obligations under these Terms and Conditions
3. If any part of these Terms and Conditions are illegal or unenforceable, we may remove that part from these Terms and Conditions and the remaining parts will continue in force

4. Accuracy of information and representations and false or misleading information

1. You understand that:

a. giving false or misleading information is a serious offence, under the *Criminal Code Act 1995* (Cth);

b. we regularly undertake audits of access to, and use of, the System; and

c. if we become aware of the provision of false or misleading or information or any fraudulent activity in connection with your Secure Access Details or the System, to the extent permitted by law, the Commonwealth will pursue the relevant person(s)

2. You agree:

a. that all information you provide, and representations you make, to us are true, complete and accurate;

b. that we are not liable for the accuracy of any information provided or representations made by you or for any action taken by us in reliance on that information or those representations, where you do not provide information that is true and correct in all respects;

c. that you must not provide false and misleading information and that doing so may result in prosecution and civil or criminal penalties;

d. to promptly notify us in the event that you consider any information provided, or representation made by you:

i. needs to be updated, including your email address as held in our records; or

ii. is or may be incorrect or misleading;

e. that we are not responsible for any failure in relation to payments made to you where you do not provide correct bank account details; and

f. that providing incorrect information through the System that results in an overpayment to you will be treated in the same way as providing incorrect information on a form or in person

5. Terms of use of the System

1. You agree:

a. that any use of the System using your Digital Credential, or any use of the System by your delegate(s), is taken to be a use of the System by you;

b. that we may monitor your access to the System;

c. that we own all intellectual property rights in the System or use the System under licence from a third party;

d. that your use of the System is by way of a non-exclusive licence as set out in these Terms and Conditions and in no way transfers or assigns ownership in any intellectual property rights (including copyright) to you; and

e. that we will use reasonable efforts to protect information submitted by you in connection with the System, but you agree that your submission of such information is at your sole risk, and we disclaim any and all liability to you for any loss or liability relating to such information in any way

6. Personal Information

1. You declare that you will comply with your obligations under the *Health Insurance Act 1973* (Cth) to not make a record of, divulge or communicate protected information (as defined in section 130 of the *Health Insurance Act 1973* (Cth)) other than in the course of your duties as a healthcare provider. You understand that failure to do so may be an offence under the *Health Insurance Act 1973* (Cth)

2. You declare that you will comply with your obligations under the *National Health Act 1953* (Cth) to not divulge or communicate protected information (as defined in section 135A of the *National Health Act 1953* (Cth)) other than in the course of your duties as a healthcare provider. You understand that failure to do so may be an offence under the *National Health Act 1953* (Cth)

3. You agree:

a. to keep Personal Information about other persons uploaded to the System by you, or accessed from the System by you, confidential;

b. not to access, use, disclose, publish, communicate, retain or otherwise deal with Personal Information except in the course of performing your duties directly related to your access to or

use of the System;

c. to store and protect Personal Information with appropriate security, having regard to the nature of the information; and

d. that your privacy obligations under clauses 6.3(a) to 6.3(c) are perpetual.

4. You understand that your Personal Information is protected by law, including the *Privacy Act 1988* (Cth) and is collected by us for the assessment and administration of payments and services
5. You understand that your Personal Information may be used by us or given to other parties for the purposes of research, investigation or where you have agreed or it is required or authorised by law
6. You understand that you can get more information about the way in which we will manage your Personal Information, including our privacy policy or by requesting a copy of the full privacy policy from us

7. Security

1. You agree:
   a. to keep:
      i. your Digital Credential;
      ii. your authentication details, password(s), passphrase(s) and tokens with respect to your PKI Digital Credential (as applicable);
      iii. your System secret questions and answers;
      iv. any mobile phone, smart phone or tablet containing an application for generating a System secure access code;
      v. any System secure access codes generated via a mobile phone application or smart phone application; and
      vi. any other security details for your access to the System, (together, your "Secure Access Details") confidential and secure whilst the item is valid for accessing the System;
   b. to take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of your Secure Access Details, which includes ensuring that your device, computer or workstation (as appropriate) being used to access the System is appropriately secured (for example, locked) when unattended;
   c. where required, to change your System password(s) regularly and when prompted by the System and/or us;
   d. to not permit any other person to use your Secure Access Details; and
   e. that you must ensure that you have appropriate business and security controls in place to ensure all claims, forms and other documentation submitted to us, whether using the System or otherwise, are appropriately authorised, and require your delegates to do the same

8. Notification to us

1. You agree to immediately notify us in writing in the event:
   a. of the possible loss or theft of any of your Secure Access Details;
   b. that you consider or suspect that any of your Secure Access Details are compromised in any way;
   c. that you become aware of or suspect that an unauthorised person:
      i. has accessed the System; or
      ii. has submitted claims, forms or other documentation to us, whether using the System or otherwise; or
      iii. that you become aware of or suspect any **identity** theft, impersonation or any other fraudulent activity in connection with your Secure Access Details or the System

9. Accessibility

1. You agree:

a. that we may from time to time change our technical requirements in relation to the use of the System, which may require you to:

b. change your Secure Access Details; or

c. upgrade your software / browser; and

d. that your access to the System is contingent on services provided by telecommunications and internet service providers, and other external factors, and that we cannot guarantee the availability of the System

10. Changes to the System

1. You agree:

a. that we may make changes to the System at any time, with or without notice to you;

b. that we may notify you of changes to the System through information and notices available to you when you access the System;

c. that you are responsible for regularly accessing notices and information provided by us through the System; and

d. that in the future, we intend to make changes to the System to link you (being an individual) to one or more health provider organisations (if applicable), with corresponding changes to these Terms and Conditions in accordance with **clause 2**

11. Subscriptions and email notifications

1. You agree:

a. that the System's Subscription service (**Subscriptions**) is a voluntary opt-in service and if you opt-in to Subscriptions, you agree you are unable to withdraw from Subscriptions for thirteen (13) weeks, and that by opting-in to Subscriptions, you will not receive paper/hardcopy statements and documents from us;

b. that the System's Automatic Subscription service (**Automatic Subscriptions**) is an automatic service through which you may be automatically subscribed to receive some statements electronically through the System, and that you cannot control access to or unsubscribe from Automatic Subscriptions; and

c. that by selecting Yes to receiving email notifications, you opt-in to be notified by email when you have new correspondence in the System's Mail Centre service (**Mail Centre**), and that you are able to opt-out of Mail Centre at any time

12. Liability

1. You agree:

a. that you are responsible for any damage to your computer, systems or software caused by any Harmful Code, corruption, attack, interference or other security intrusion;

b. that to the maximum extent permitted by law:

i. we make no warranty, express or implied, that the information included in or accessed through the System is correct or current;

ii. the System is provided on an 'as is' and 'as available' basis and we make no representations or warranties that the System will be free from loss, corruption, attack, Harmful Code, interference or other security intrusion, or will be uninterrupted, error free, fit for purpose, that any defects with the System will be rectified or that the System will not have unintended effects on the operation of your computer, systems or software;

iii. we (and our employees and agents) exclude any and all liability we (or they) may have to you or anyone acting on your behalf for any claims, costs, losses, liabilities, expenses or damage ("Losses"), whether direct, indirect or consequential, punitive, special or otherwise (including, without limitation, communication costs, support costs, software acquisition or losses including losses associated with the System being from time to time inoperative or inaccessible) arising from or in connection with:

A. your access to or use of, or anyone on your behalf's access to or use of, the System;

B. errors or omissions in content;

C. incorrect information provided to you;

D. your failure to comply with these Terms and Conditions;

E. our termination or suspension of your access to the System;

F. your loss or disclosure of your Secure Access Details; and

G. the System being altered or modified or not being available

13. Restriction, suspension and termination

1. You agree:
   a. that we may at any time, at our absolute discretion, restrict or suspend your access (including access of any of your delegates) to the System, including:
      i. because we reasonably believe that you have breached these Terms and Conditions;
      ii. because you have been removed from the Register;
      iii. because we reasonably believe that your access has been used to perform an unauthorised transaction;
      iv. because you are no longer eligible to access the System; or
      v. for any other reason;
   b. that we may at any time, at our absolute discretion, terminate your access (including access of any of your delegates) to the System, including:
      i. because we reasonably believe that you have breached these Terms and Conditions;
      ii. because you have been removed from the Register;
      iii. because we reasonably believe that your access has been used to perform an unauthorised transaction;
      iv. because you are no longer eligible to access the System; or
      v. for any other reason;
   c. that either party may terminate these Terms and Conditions at any time by giving written notice to the other party (**Date of Termination**). You understand that you will not be able to use the System after termination however, any rights we may have in respect of your use of our System are preserved; and
   d. that if these Terms and Conditions are terminated, your obligations under these Terms and Conditions will continue in respect of any use of the System before the Date of Termination, and our rights to recover any debt owing will also continue

14. Jurisdiction

1. These Terms and Conditions are issued under and are to be construed in accordance with the laws in force from time to time in the Australian Capital Territory. All parties submit to the non-exclusive jurisdiction of the courts of the Australian Capital Territory and courts of appeal from them. Neither party will object to the exercise of jurisdiction by those courts on any basis

15. Contra Proferentem

1. No rule of construction will apply in the interpretation of these Terms and Conditions to the disadvantage of one party on the basis that that party put forward or drafted these Terms and Conditions or any part of these Terms and Conditions

16. Contact Information

1. If you have any questions about these Terms and Conditions, please contact us

17. Declaration

1. By clicking "I agree" and submitting this document, You declare that:
   a. you have the authority to agree to and submit this document;

b. the information provided is true, complete and correct;

c. you have read and understood the Terms and Conditions as outlined in clauses 1 to 18;

d. you have read and understood the AIR Terms and Conditions as outlined in clause 19; and

e. you are the individual that you assert to be

18. Definitions and interpretation

1. In these terms and conditions, a reference to:

   a. "**AIR**" means the Australian Immunisation Register established and kept under the *Australian Immunisation Register Act 2015* (Cth);

   b. "**AIR Terms and Conditions**" means the AIR terms and conditions as set out in **clause 19**, as amended from time to time in accordance with **clause 2**;

   c. "**Digital Credential**" means:

      i. a unique PRODA digital credential assigned to an individual, for access to the System, comprised of a username and password(s); or

      ii. a unique authentication assigned to an individual or organisation through the use of a DHS PKI certificate, for access to the System;

   d. "**Harmful Code**" means any software or code that is designed to infiltrate a device, computer or system without a user's informed consent, such as malware, virus, hacking tools and Trojans, irrespective of the origin;

   e. "**HPOS**" means the Health Professional Online Services system, which includes access to a range of programs including the Medicare Bulk Bill Webclaim, DVA Webclaim and DVA Allied Health Webclaim;

   f. "**Human Services**" means the Commonwealth of Australia acting through the Department of Human Services;

   g. "**Personal Information**" has the same meaning as under section 6(1) of the *Privacy Act 1988* (Cth) which is, information or an opinion about an identified individual, or an individual who is reasonably identifiable:

      1. whether the information or opinion is true or not; and

      2. whether the information or opinion is recorded in a material form or not;

   h. "**PKI**" means Public Key Infrastructure, and refers specifically to Human Services' electronic trust framework to provide authentication and confidentiality for online transactions through the use of keys and certificates;

   i. "**PRODA**" means the Provider Digital Access system;

   j. "**Register**" means the Australian Health Practitioner Regulation Agency Register of Practitioners;

   k. "**Secure Access Details**" has the meaning given in clause 7.1(a);

   l. "**Service Supplier**" means:

      i. Human Services;

      ii. the Chief Executive Medicare; and/or

      iii. the System Operator of the My Health Record system appointed under section 14 of the *My Health Records Act 2012* (Cth);

   m. "**System**":

      i. HPOS; and

      ii. where clause 19 applies, includes AIR; and

   n. "**System Operator**" means Human Services, which provides an online interface to the systems of the Service Supplier

2. In these Terms and Conditions:

   a. headings are for convenience only, and do not affect interpretation;

   b. a singular word includes the plural, and vice versa;

   c. a reference to a clause is to a clause in these Terms and Conditions; and

   d. the meaning of general words is not limited by specific examples introduced by "including", "for example" or similar expressions

19. AIR Terms and Conditions

1. These AIR terms and conditions apply (in addition to the clauses of the HPOS Terms and Conditions) when I access and use AIR through HPOS. Noting:
    a. Section 4 of the *Australian Immunisation Register Act 2015* (`the Act') defines protected information as meaning personal information, relevant identifying information or information that is commercial in confidence, to the extent that this information:
        i. is obtained under, or in accordance with, the Act; or
        ii. is derived from a record of information that was made under, or in accordance with, the Act; or
        iii. is derived from a disclosure or use of information that was made under, or in accordance with, the Act
    b. It is an offence, punishable on conviction by imprisonment or a fine, for a person, while unauthorised to do so, to disclose or use any protected information
2. I acknowledge that:
    a. I am a recognised vaccination provider or a prescribed body for the purposes of the *Australian Immunisation Register Act 2015*
    b. I may collect, make a record of, disclose or otherwise use protected information only for the purposes of the AIR
3. I agree to:
    a. Not make a record of, disclose or otherwise use protected information other than for the purposes of the AIR or as required or authorised by law or Court or Tribunal order;
    b. Take active measures to ensure the security of any protected information;
    c. Take reasonable steps to protect any protected information from misuse, interference and loss, as well as unauthorised access, modification or disclosure;
    d. Comply, as far as practicable, with any policy guidelines laid down by the Commonwealth or issued by the Office of the Australian Information Commissioner in relation to the handling of any protected Information;
    e. Undertake any specific privacy training required by the Commonwealth related to the handling of protected information so that I am aware of the obligations imposed by relevant privacy laws and the *Australian Immunisation Register Act 2015*;
    f. Ensure that persons under my direction or control, who will access any protected information, undergo privacy training so that they are aware of the obligations imposed by relevant privacy laws and the *Australian Immunisation Register Act 2015*;
    g. Immediately notify the Commonwealth upon becoming aware of a breach or possible breach of any of the obligations contained in, or referred to in paragraphs **a – f** above; and
    h. The obligations under paragraphs **a – g** above apply in perpetuity
4. I declare that I have read and agree to comply with the Human Services' privacy policy

20. Department of Veterans' Affairs (DVA) Terms and Conditions

1. I agree and certify that no charge will be levied against the patient/s for the service/s

Page last updated: 27 August 2017