AMA

Privacy and Health Record Resource Handbook

For Medical Practitioners in the Private Sector

Published by AMA, Canberra, 2017

The Privacy and Health Record Resource Kit is based on the Privacy Resource Handbook, 2010. The law stated herein is applicable as of June 2017.

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 introduced significant changes to the Privacy Act, in 2014. Since the, further changes, including the Privacy Amendment (Notifiable Data Breaches) Act 2017 have led to this update of the Handbook.

The changes introduce an obligation on entities regulated by the Privacy Act to notify individuals and the Commissioner of a serious breach. This is explained in more detail in the Handbook.

We have included other useful information and resources as well, such as a risk assessment tool, and further notices for use in medical practices.

The AMA welcomes updates and enhancements to privacy legislation, and it is to that end that we provide this Handbook to assist medical practices to understand and implement their responsibilities in regard to privacy and patient records.

October 2017

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 Handbook 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 Handbook aimed at?

This Handbook is aimed at medical practitioners in the private sector who are subject to the Commonwealth Privacy Act (1988). Those working in public sector institutions should consult their health authority's privacy policies and State or Territory privacy legislation.

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. 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 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 includes organisations that provide health services[1]

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 with 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.

[1] Privacy Act 1988 (Cth) ss6, 6C, 6D

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 located overseas, or which will use overseas servers or other resources. 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.

Law enforcement

Using or disclosing personal information for an enforcement related activity

You may disclose personal information for a secondary purpose where you reasonably believe that the use or disclosure of the personal information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e)). This includes the police. Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities. When in doubt, if police are requesting information, you should ask for authority from a senior officer.

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. It may also apply if you are using 'data transcription' or other service that requires patients' records to be disclosed overseas. 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.

There is a basic tension here between the long standing practice of many doctors to retain records indefinitely, and destroying those no longer needed as required by APP 11. The key here is to determine when records are genuinely no longer needed. This is really a judgment call for each practice, but you should be certain a patient's records are no longer current (that patient has not consulted you for a significant amount of time) and you would not be contravening State or Territory health record laws regarding retention (basically 7 years from the last consultation for adults and up to the age of 25 for children).

However, if you have contentious files (that might, for example, give rise to litigation), they may still be required for a significant period of time and the AMA would suggest that you should retain those records until you are absolutely certain they are no longer needed. There are many reasons patients may want to access their records. One of those may be to sue another party for personal injury. Retaining the records for at least 7 years will generally cover the basic limitation period for personal injury in most jurisdictions.

Before destroying or deleting any file, it would be prudent to contact the patient concerned (if possible) and advise them that you intend to destroy their health record, and give them the chance to retrieve it. In any event, when you do destroy or delete a health record, in some States and Territories there are certain obligations you should be aware of. Broadly, you should keep a record of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted or disposed of.[2]

<u>De-identifying data</u>
APP 11 also allows for 'de-identification' of data held by your practice. Occasionally you may be required, or we you consider it beneficial, to provide certain data to agencies such as government agencies or research organisations. This is usually for research or statistical purposes.

<u>What is de-identification?</u>
Personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

For example, you may provide information on the number of female and male patients you have, but without providing the details of any individual. In this simple example no personal information or sensitive information is disclosed. No privacy law is breached.

De-identification involves removing or altering information that identifies an individual or is reasonably likely to do identify an individual. Generally, it includes two steps:

- removing personal identifiers, such as person's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

De-identification can be effective in preventing re-identification of an individual, but may not remove that risk altogether. 'Re-identification' occurs when individuals are able to be identified from previously de-identified

[2] See, for example, Health Records and Information Privacy Act 2002 (NSW), s25(2)

data. This may be where other information could be matched with the de-identified information, or de-identified information is so specific that it is able to be matched to an individual.
Before you provide any de-identified data, you should assess the risks of 're-identification' according to the guidelines issued by the Office of the Australian Information Commissioner and do not provide any information where you assess that there is a risk of 're-identification', unless you are required to do so by law.

If de-identification is done successfully, the information that is de-identified will no longer be 'personal information' because it will not be 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[3]

We have provided a notice at the end of this kit that you can use to alert your patients to the fact that parts of their health record may be used as de-identified data.

[3] Privacy Act 1988 (Cth) s6

Case note

Pound Road Medical Centre, July 2014

On 13 December 2013, the Australian Privacy Commissioner (the Commissioner) opened an investigation into the operator of a medical centre ('the operator'). This was in response to media reports that there were boxes of unsecured medical records at a site it had occupied.

The operator relocated its practice in 2011. It advised the OAIC that since November 2004 it had computerised all patients' health records and believed that all the paper-based health records stored at the site were transferred to a locked store at their new premises and later to a garden shed off site. It seems at some stage this shed had been breached.

It was estimated that approximately 960 patients' personal information was compromised in the data breach. The operator clarified that the majority of the health records compromised related to individuals who ceased to be active patients of the medical practitioner who conducted the practice prior to 2004.

As the event occurred in 2013, the matter was decided under the ten National Privacy Principles (NPPs), which were replaced by the Australian Privacy Principles (APPs) on 12 March 2014.[1]

Security of personal information

The Commissioner found that more stringent steps were required of the operator to keep their information secure than may be required of organisations that do not handle sensitive information. The operator failed to meet the requirement under the Privacy Act to keep the sensitive information it held secure. The Commissioner considered operator's storage of health and other personal information records in a garden shed, particularly at premises it no longer operated or staffed, to be a failure to take reasonable security steps.

Secure destruction or de-identification of personal information

NPP 4.2(Now APP 11.2) required organisations to take reasonable steps to destroy or permanently de-identify personal information not being used or no longer required.

The majority of the operator's records were at least eleven years old, which also indicated a failure by it to identify and securely destroy or de-identify personal information that was no longer being used or required.

The Commissioner considered that prior to the data breach the operator failed to take reasonable steps to destroy or permanently de-identify personal information it held that was no longer in use or needed.

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.

<u>Exceptions to access</u>

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.

16B (1A) A permitted health situation exists in relation to the collection by an organisation of health information about an individual (the third party) if:

(a) it is necessary for the organisation to collect the family, social or medical history of an individual (the patient) to provide a health service to the patient; and

(b) the health information about the third party is part of the family, social or medical history necessary for the organisation to provide the health service to the patient; and

(c) the health information is collected by the organisation from the patient or, if the patient is physically or legally incapable of giving the information, a responsible person for the patient.

This means you can collect a patient's family history for clinical purposes without breaching privacy. (This was previously allowed under Public Interest Determination 12, no longer in force and no longer necessary due to the inclusion of the above section in the Privacy Act).

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.

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.

See:https://www.humanservices.gov.au/health-professionals/enablers/accessing-prescription-shopping-information-service-hpos

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.

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

My Health Records Act 2012

The *My Health Records Act 2012* (MHR Act) controls the collection, use and disclosure of information in an individual's My Health record. Contravention of the MHR Act is an interference with privacy and for the purposes of the *Privacy Act 1988*, an interference with the privacy of a healthcare recipient.[4]

Special Areas of Concern

Who owns the medical records I create?

Patients often have the view that their medical records 'belong' to them. As a general rule, the doctor who holds patient information owns and controls it. That is, ownership of the physical property in the records.

The patient has a right, generally speaking, to access health records created in relation to them. You need to be careful in situations where doctors are working under contract to practices to make it clear who owns the records. Generally speaking the 'owner' will have responsibility for compliance with the Privacy Act, but in reality a doctor working under contract in a practice may rely on administrative staff to oversee most day to day record handling and will rely on them to comply with privacy obligations. It should be noted, however, that ultimately if a breach occurs (see further below under 'Data Breaches') the doctor who owns the records is likely to be held responsible.

Copyright

Copyright in the information within them is a bit more complex. Medical records may be comprised of a range of documents including health summaries, doctors' notes, referral letters, diagnostic images, prescriptions etc. Copyright may subsist in works with sufficient intellectual effort, such as referral letters but not in things like simple prescriptions. [5]

The copyright of specialists' reports held on a GP's file belongs to the specialist who wrote the report.

[4] My Health Records Act 2012 (Cth) s73

[5] See: *Primary Health Care Ltd v Commissioner of Taxation* [2010] FCA 419

If challenged, the issue of copyright would have to be analysed on a case by case basis.

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, where it is protected by copyright. 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.

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 request a court to impose a civil penalty of up to $1.7 million for an organisation found to be in serious or repeated breach of the Privacy Act.

Most determinations by the Privacy Commissioner attract several thousand dollars in settlement (compensation) for the person whose privacy has been breached

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.

Medical practices and bad debt

All medical practices encounter patients who won't pay their bills. Normally letters of demand are in order. It is prudent to get legal advice on this before proceeding with any action to recover a debt that involves going further than this or giving a patient's details to a 'collection agency'.

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 would reasonably be expected, but chasing up non-payment requires more care.

Patients would reasonably expect doctors to chase unpaid accounts. However, it is not generally permissible to disclose a patient's name and address to a debt collection agency to recover a bad debt, unless it is clear that the practice is a 'credit provider'. That means they have extended credit to the patient in respect of the provision of goods or services on terms which allow the deferral of payment, in full or in part, for at least 7 days.[6] This should be made clear on invoices.

When in doubt, contact the OAIC for further clarification, or seek legal advice before listing a patient's debt with a collection agency.

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

[6] Privacy Act 1988 (Cth) s6G

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 health service provider argued it was a credit provider (under a previous Determination no longer in force) because it provided a loan and that loan was not paid within 7 days even though its invoice did not explicitly state that immediate payment was required.

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.

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 found that the health service provider had taken some steps to ascertain whether it was a credit provider. However, given the potentially serious financial consequences of listing the payment default, the Commissioner considered further steps were necessary, such as seeking legal advice or contacting the Commissioner's Office.

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. This should generally be approached with advice from experts in the field.

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. This will usually require production of a parenting order or agreement. 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, if you are able to do so.

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.

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.

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,[7] 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.

[7] Privacy Act 1988 (Cth) APP 12

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.***

Privilege, evidence and confidential communications

Legal processes and privacy

As we have previously noted, the Privacy Act allows you to disclose patient records in certain situations in pursuing a legal claim. There are other processes and legislation that impact on this. Litigation is a complex process which can be different in every jurisdiction. It is beyond the scope of this paper to cover all possible situations regarding health records and legal processes but we offer a brief overview to guide you. In all cases, where you have doubts about what to do, you should seek advice from your local AMA, your indemnity insurer, or a legal advisor.

Pre trial discovery (or disclosure)

The process of pre-trial discovery allows parties to obtain documents from the other side in litigation before a trial starts. If you are party to litigation (for example, a patient is suing you), you should seek legal advice immediately regarding the process of pre-trial disclosure.

Where you are asked to write a report regarding a patient but you are not a party to proceedings, you should clarify with the party commissioning the report whom it should be disclosed to.

The law of privilege

The law of privilege accords individuals the right to resist disclosure of confidential information. Generally the common law affords no protection to communications made in the course of the professional confidential relationships between doctor and patient.

However, legislation in a number of jurisdictions has extended the doctrine of privilege to other confidential relationships. There now exist in some jurisdictions limited privileges in respect of medical communications and sexual assault communications.

The *Evidence Act* in certain jurisdictions allows a court to direct that evidence not be adduced in a proceeding if the court finds that adducing it would disclose a protected confidence, or the contents of a document recording a protected confidence. This applies to a communication made by a person in confidence to a confidant in the course of a relationship in which the confidant was acting in a professional capacity.

This is a discretionary power of a court to direct that evidence not be presented in a proceeding if it would disclose communications subject to the privilege. It only applies to communications made by the client and not by the confidant (so the patient's communications – it is unlikely to cover all of the health record). It only applies to judicial proceedings and not to an authority exercising a statutory information gathering power (see below for other situations).

Some Evidence Acts are a little stronger (such as s127A of the Evidence Act 2001 (TAS)) and provide that a medical practitioner must not, without the consent of their patient, divulge in any civil proceeding any communication made to him or her in a professional capacity by the patient. Again, this does not necessarily apply to the whole record – only communications made by the patient.

Normally a party is obliged to include privileged documents in their 'List of Documents' and claim privilege over them as appropriate. In some circumstances, privilege may be asserted, and objected to by the other party to litigation. A legal advisor should guide you through this.

<u>Sexual assault communications privilege (SACP)</u>
This mostly applies in criminal matters but can also apply to civil proceedings by the operation of Evidence Acts in various jurisdictions. You should be aware of it if you have dealt with patients who are victims of sexual assault.
It limits the disclosure in court of counselling, health and other therapeutic information about a victim of sexual assault. If you are asked to produce these notes you should seek legal advice.
This does not normally mean you can withhold evidence in legal proceedings – it means a court may decide that evidence can't be used. You should discuss this with a legal advisor. (see below re objecting to producing documents).

<u>Subpoenas and other third party notices</u>
In all states a valid subpoena or summons generally overrides your duty of confidentiality and privacy to the patient and should be complied with. If you have doubts about its validity you should check with the court that issued it or a legal advisor.

Subpoenas will generally require you as a person not a party to proceedings to produce documents or appear as a witness. Where you are required to produce documents to a court. You should do so (usually copies are allowable but check the subpoena for details) by the date noted on the subpoena.

<u>Discovery of documents from non-parties</u>
A notice of non-party disclosure is a court document requiring you to produce records that are directly relevant to an issue in legal proceedings. The records can be produced for inspection by the applicant or their solicitor. Generally you must comply with these, but if you believe there is a valid reason to object, seek legal advice immediately.

<u>Objections to producing documents</u>
In limited circumstances you can object to producing records in answer to a subpoena, summons or notice of non-party disclosure. The grounds for objection include matters such as a communication that would fall within confidential communications relationship privilege or sexual assault communications privilege. If you do wish to object to producing records under a subpoena, you should only do so on legal advice.

Other situations of disclosure

There are also situations in which health records of a person who is not a party to obtained, by means other than a subpoena. This may happen, for example, in health practitioner disciplinary cases involving a complaint against a medical practitioner, where that practitioner must appear before a panel or tribunal and health records of their patients may be disclosed in proceedings. Health practitioners must comply with requests for medical records in these circumstances unless there is a very good reason not to. If, for example, the records requested were not relevant to proceedings, you should raise this with the authority concerned.

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. Do not assume that the patient agrees to have their health record transferred to the incoming practitioner (see case note below). 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 required. 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 necessary. 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

Data Breach Notification Scheme

The Privacy Amendment (Notifiable Data Breaches) Act 2017 amends the Privacy Act 198 (Cth) and establishes a mandatory data breach notification scheme in Australia.

It requires businesses covered by the Privacy Act (such as medical practices) to notify any individuals affected by a data breach **that is likely to result in serious harm**. The Office of the Information Commissioner (OAIC) will be advised of these breaches, and can determine if further action is required. The law also gives the OAIC the ability to direct an agency or business to notify individuals about a serious data breach.

The legislation considers a ***serious breach*** to have occurred when there is unauthorised access to, disclosure or loss of customer information held by an entity, which generates a *real risk of serious harm* to individuals involved.
An eligible data breach will occur where :

- there is unauthorised access to or disclosure of information and a reasonable person would conclude that access or disclosure would be likely to result in ***serious harm*** to any of the individuals to whom that information relates; or
- information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in ***serious harm*** to any of the individuals to whom that information relates.

Data breaches occur in a number of ways. Some examples include:

- lost or stolen laptops, storage devices, or paper records containing personal information
- hard disk drives and digital storage media being disposed of or returned to equipment suppliers without the contents first being erased
- databases being 'hacked' into or otherwise illegally accessed
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure disposal bins
- a practice mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving a practice into improperly releasing the personal information of another person.

Medical practices should put in place security safeguards that include maintaining physical security, computer and network security, communications security and personnel security. These may include:

- **Risk assessment** – Identifying the security risks to personal information held by your practice and the consequences of a breach of security.
- **Privacy impact assessments** – Evaluating the degree to which proposed or existing information systems align with good privacy practice and legal obligations.
- **Policy development** – Developing a policy or range of policies that implement measures, practices and procedures to reduce risks to information security.
- **Staff training** – Training staff in relevant procedures and codes of conduct.
- **The appointment of a responsible person or position** – Creating a designated position to deal with data breaches.
- **Technology** – Implementing privacy enhancing technologies to secure personal information held by the practice.
- **Monitoring and review** – Monitoring compliance with the security policy, periodic assessments of new risks and the adequacy of existing security measures.

- **Appropriate contract management** – Conducting appropriate due diligence where services (especially data storage services) are contracted.

What are affected entities required to do?

The new legislation places various obligations on entities in response to an eligible breach. These include:

- Assessing whether there are reasonable grounds to believe an eligible data breach has occurred within 30 days of developing a suspicion of such a breach;
- Once an entity has reasonable grounds to believe there has been an eligible data breach, prepare a statement setting out the contact details of the entity, the nature of the breach and steps it recommends affected individuals take in response. A copy must also be provided to the OAIC; and
- Taking such steps as are reasonable in the circumstances to notify affected and at risk individuals of the contents of the statement as soon as is practicable.

The OAIC may also direct an entity to notify affected individuals if it becomes aware that there are reasonable grounds to believe that the entity has suffered an eligible data breach.
Reasonable steps (as required by APP 11) necessary to secure personal information will depend on context, including (but not limited to):

- the sensitivity (having regard to the affected individual(s)) of the personal information held
- the harm that is likely to result to individuals if there is a data breach involving their personal information
- the potential for harm (in terms of reputational or other damage) to the agency or organisation if their personal information holdings are breached, and
- how the agency or organisation stores, processes and transmits the personal information (for example, paper-based or electronic records, or by using a third party service provider).

Responding to data breaches: four key steps

There are four key steps to consider when responding to a breach or suspected breach:
Step 1: Contain the breach and do a preliminary assessment
Step 2: Evaluate the risks associated with the breach
Step 3: Notification
Step 4: Prevent future breaches

Step 1: Contain the breach and do a preliminary assessment
Take whatever steps possible to immediately contain the breach.
For example, stop the unauthorised practice, recover the records, or shut down the system that was breached.
Step 2: Evaluate the risks associated with the breach
To determine what other steps are immediately necessary, you should assess the risks associated with the breach, including:

a. The type of personal information involved.
b. The context of the affected information and the breach.
c. The cause and extent of the breach.
d. The risk of serious harm to the affected individuals.
e. The risk of other harms.

Step 3: Notification
You should consider the particular circumstances of the breach, and:

a. decide whether to notify affected individuals, and, if so
b. consider when and how notification should occur, who should make the notification, and who should be notified
c. consider what information should be included in the notification, and
d. consider who else (other than the affected individuals) should be notified.

The challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

Step 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

This plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).

Reporting breaches

Reporting a breach does not preclude the OAIC from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or on the Commissioner's initiative).

What to put in a notification to the OAIC

Any notice provided to the OAIC should not include personal information about the affected individuals. It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response the agency or organisation has made to the breach
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person, and
- whether the breach has been notified to other external contact(s).

This is an overview only. For further information, see https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

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.

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: ……./……./……

De-identified data notice

This practice has developed a policy to protect patient privacy in compliance with the Privacy Act 1988 (Cth) ('the Privacy Act') and in line with the Australian Privacy Principles (APPs) in its collection, storage and use of your personal information (including your health information).

Unless we are required to by law (as with agencies such as Medicare), we will not provide your personal information without your permission. We may, however, provide **de-identified** data collected in the course of providing your medical care to government agencies or research organisations in order to in to better inform health policy and enhance quality health care.

For more information about our Privacy Policy please ask our receptionist for a copy or refer to our website.

Sample Privacy Policy

The AMA has produced, in conjunction with the Office of the Australian Information Commissioner, a sample privacy policy that may be useful to your practice. Please see supplementary document at:

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