### Sample Privacy Policy

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

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

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

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

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

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

**1. Introduction**

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

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

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

**2. What kinds of personal information do we collect?**

The type of information we may collect and hold includes:

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

**3. How do we collect and hold personal information?**

We will generally collect personal information:

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

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

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

* to provide health services to you
* to communicate with you in relation to the health service being provided to you [***Note*** re direct marketing: –sensitive information can only be used for direct marketing if consent has been given. Consent may be implied in certain circumstances. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the practice. If you do intend to communicate with patients via direct marketing with their consent, make it clear that the patient may opt out of direct marketing at any time by notifying your practice, and let them know they can do that by sending the practice a letter or email and provide the contact details for them to do so. The AMA recommends caution in relation to direct marketing and medical practices, and you may like to seek independent advice before engaging in direct marketing with patients].
* to comply with our legal obligations, including, but not limited to, mandatory notification of communicable diseases or mandatory reporting under applicable child protection legislation.
* to help us manage our accounts and administrative services, including billing, arrangements with health funds, pursuing unpaid accounts, management of our ITC systems
* for consultations with other doctors and allied health professional involved in your healthcare;
* to obtain, analyse and discuss test results from diagnostic and pathology laboratories
* for identification and insurance claiming
* [***Note***: If your practice uses the My Health Record system]: If you have a My Health Record, to upload your personal information to, and download your personal information from, the My Health Record system.
* [***Note***: If your practice uses an electronic transfer of prescriptions service - you will need to specify if your practice participates in this service]: Information can also be disclosed through an electronic transfer of prescriptions service.
* To liaise with your health fund, government and regulatory bodies such as Medicare, the Department of Veteran's Affairs and the Office of the Australian Information Commissioner (OAIC) (if you make a privacy complaint to the OAIC), as necessary.

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

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

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

We will normally respond to your request within 30 days.

**6. How do we hold your personal information?**

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

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

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

**7. Privacy related questions and complaints**

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

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

**Phone:** 1300 363 992

**Email:** enquiries@oaic.gov.au

**Fax:** +61 2 9284 9666

**Post:** GPO Box 5218
Sydney NSW 2001

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

**8. Anonymity and pseudonyms**

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

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

**9. Overseas disclosure.**

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

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

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

overseas based cloud storage [***Note***: you need to be aware that privacy and cloud based storage services can be a complex issue. For example, if you use an overseas based cloud-storage service provider but the information is encrypted to the point where the cloud service provider cannot access it, but merely stores it, then it is likely that the practice will be considered to be holding and using that personal information and not disclosing it to the cloud service provider. However, if the cloud service provider can access and collect the information, this is likely to be an overseas ‘disclosure’ on the part of the practice. If in doubt, it is best to consider the use of cloud based storage services as a ‘disclosure’. For more information, see: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>]

* anyone else to whom you authorise us to disclose it

**10. Updates to this Policy**

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

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

**11. Privacy and websites**

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

**12. Contact details for privacy related issues**

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

1. See: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home [↑](#footnote-ref-1)