RACGP

Royal Australian College *of* General Practitioners

Privacy and managing health information in general practice

The Royal Australian College of General Practitioners (RACGP) has developed a privacy policy template for general practices to adapt, for compliance with the requirements of the Australian Privacy Principles (APPs). It is important each practice uses this template as a guide and adapts its content to their individual procedures.

This template covers:

- practice procedures
- staff responsibilities
- patient consent
- collection, use and disclosure of information
- access to information.

The template is designed to communicate to patients how a practice manages personal information and to complement other practice policies such as complaint resolution and breach notification procedures. The sections in red text are for you to revise and adapt to the specific procedures of your general practice.

This template was developed with assistance from the Office of the Australian Information Commissioner (OAIC) and was current at time of publication.

For more information on privacy visit www.oaic.gov.au, or for privacy policies for GPs, visit www.oaic.gov.au/privacy/privacy-resources/training-resources/privacy-policies-for-gps

Make your policy freely available for your patients so they know that it exists and they can access it. For example, display it at your practice reception and on your website if you have one, and make reference to it in your registration forms and other forms or notices.

This policy should be reviewed regularly to ensure it remains applicable to current practice procedure and legal requirements.

[Insert practice name] privacy policy

Current as of: [insert date of last revision]

Introduction

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties.

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

[Note: Make sure your patient registration form or other process includes a section for patients to provide consent.]

Why do we collect, use, hold and share your personal information?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- health fund details.

Dealing with us anonymously

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.

[Note: The *Privacy Act* requires you to provide patients with the option of not identifying themselves, or of using a pseudonym, when dealing with you (APP 2) unless it is impracticable for you to do so. Information about this should appear in the practice privacy policy or collection notice.]

How do we collect your personal information?

Our practice may collect your personal information in several different ways.

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.

   [Your practice should have a collection statement attached to/within the patient registration form.]

2. During the course of providing medical services, we may collect further personal information.

   [Information can also be collected through electronic transfer of prescriptions (eTP), My Health Record, eg via Shared Health Summary, Event Summary. You will need to specify if your practice participates in any of these eHealth services.]

3. We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.

   [Consider whether this applies to your practice and amend as appropriate.]

4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:

   - your guardian or responsible person
   - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
   - your health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

When, why and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties who work with our practice for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers
- when it is required or authorised by law (eg court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (eg via Shared Health Summary, Event Summary).
  [You will need to specify if your practice participates in any of these eHealth services. Are there any other usual disclosures specific to your practice which you should include here?]

Only people who need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

[Alternatively, if your practice is likely to share personal information outside of Australia, clearly set out where you are likely to make those disclosures if it is practicable to do so, eg if you are using overseas transcription services you will need to make your patients aware of this. If you are not sending information overseas, state this clearly.]

Our practice will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying our practice in writing.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms.

[Specify the ways in which your practice stores information, eg as paper records, electronic records, visual records (X-rays, CT scans, videos and photos), audio recordings.]

Our practice stores all personal information securely.

[Explain how you securely store and protect personal information, eg electronic format, in protected information systems or in hard copy format in a secured environment. Provide specific examples such as your

use of passwords, secure cabinets, confidentiality agreements for staff and contractors. However, you should not provide details that would jeopardise the effectiveness of your security measures.]

How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing [specify how your practice will receive such requests] and our practice will respond within a reasonable time. [Insert a reasonable timeframe specific to your practice processes, eg 30 days is generally considered reasonable. Also provide details of any fees that may be associated with providing this information if applicable – these must not be excessive. Patients cannot be charged for making the request – only for the costs of complying with the request].

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by our practice is correct and current. You may also request that we correct or update your information, and you should make such requests in writing to [insert your specific contact information of practice/practice manager, eg an email address].

How can you lodge a privacy-related complaint, and how will the complaint be handled at our practice?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure. [Provide contact details of your practice, such as an email address. You must include your mailing address and contact number. Insert turnaround timeframe specific to your practice processes, eg 30 days and any other key provisions of your complaint handling process.]

You may also contact the OAIC. Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992. [You could also provide details to contact your relevant state or territory health authorities/ombudsman, if they also have jurisdiction.]

Privacy and our website

[Note: This section is optional. If you are collecting personal information via your practice website or interact with your patients digitally (eg through social media or by email) you need to include a statement about the collection of personal information that occurs through the website or social media and the use of website analytics, cookies, etc.]

Policy review statement

[State that this privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. State how you will notify your patients when you amend this policy.]