



# Privacy Requirements and Patient Data Compliance for General Practice

October 2018

**Magali De Castro**  
Clinical Director, HotDoc

---

---

# Privacy Requirements and Patient Data Compliance for General Practice

This session will cover:

---

- An overview of the Australian Privacy Principles as they apply to General Practice
- How and when to request and document patient consent for the use of their personal or clinical information
- What services patients have the right to opt-in and opt-out of
- What practices can and cannot use patient data for
- What should be included in a practice's Privacy policy and how this should be communicated to patients

---

# What do we mean by Privacy?

## Collecting & using sensitive information

---

Most of the information we collect in General Practice is sensitive information.

Under the Privacy Act, sensitive information has more strict requirements.

We can **only collect sensitive information with consent.**

The way we manage information & privacy has to be in line with the **Australian Privacy Principles (APPs)**, which came in effect in 2014.

---

# Australian Privacy Principles (APP)



13 APPs apply to all organisations

**APP 1** - Open and transparent management of personal information  
(Clear and easily accessibly Privacy Policy)

**APP 2** - Anonymity and pseudonymity

**APP 3** - Collection of solicited personal information

**APP 4** - Dealing with unsolicited personal information (e.g. correspondence received for a person who is not a patient of the practice)

**APP 5** - Notification of the collection of personal information

**APP 6** - Use or disclosure of personal information (e.g. IT, Accreditation, My Health Record, Australian Immunisation Register, etc.)

---

# Australian Privacy Principles (APP)



13 APPs apply to all organisations

**APP 7** - Direct marketing (e.g. Patient opt-in & opt-out)

**APP 8** - Cross-border disclosure of personal information (e.g. Overseas services)

**APP 9** - Adoption, use or disclosure of government identifiers (e.g. Medicare number, My Health Record)

**APP 10** - Quality of personal information (e.g. Accurate & current)

**APP 11** - Security of personal information

**APP 12** - Access to personal information

**APP 13** - Correction of personal information

---

## In a nutshell: Privacy points for consideration

Be mindful & inform your patients about how the practice:

**Collects** their personal and health information

**Uses** their information for clinical & administrative purposes

**Shares** their information (e.g. other clinicians, services such as IT, Accreditation or Government Agencies, such as when using My health Record or the Australian Immunisation Register)

**Disposes** of information when no longer needed

**Gives patients access to their information**

**Gives patients access to the privacy policy**

**Informs patients about** your processes regarding **direct marketing**

---

# What practices can and cannot use patient data for

## In most cases:

A practice is only permitted to use the health information of a patient or disclose to third parties (such as IT providers, accreditation agencies or other contractors) if:

- Your patients have **consented to this use or disclosure**; or
- Your patients would **reasonably expect you to use or disclose their information for this purpose** (and it is **directly related to the primary purpose** of you having collected it e.g. to provide them with clinical care).

---

## Other factors affecting privacy



### Physical layout of the practice

A carefully physical layout can help privacy and confidentiality.

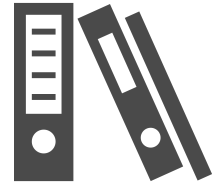
For example:

- Having good sound proofing between internal walls
- Adequate private areas for private conversations
- Make sure computer screens in reception are hidden from the view of patients and visitors (password protection & screen savers)
- Make sure private and confidential discussions in the reception cannot be easily overheard



---

# How does your practice approach privacy?



Good strategies include:

- Having a **clear, transparent and patient-friendly** privacy policy
- Having a **key staff member** (usually the practice manager) in charge of overseeing privacy procedures and training other staff
- Having a consistent staff **training** approach to privacy & confidentiality
- Have all staff sign **confidentiality agreements** and store them in the staff files

---

# How and when to request and document patient consent for the use of their personal or clinical information

- As soon as possible/practical, ideally using a range of methods and as part of your usual patient-practice workflow
  - *New patient registration form* (paper or electronic)
  - Practice **information sheet**
  - Practice **website** (online booking, privacy policy link, etc.)
  - Practice **reception/waiting room signage** to inform about privacy policy and how to access this (online, via reception)
  - **In person** by reception or clinical staff

**Note:** For electronic forms, you may use electronic signatures or a checkbox the patient has to tick to agree to your terms of service.

---

# Considerations when sending commercial electronic messages (Direct Marketing)

The Spam Act (2003) regulates the sending of commercial electronic messages.

This includes communication by:

- Email
- Mobile (SMS or text messages)
- Multimedia message service (MMS)
- Instant messaging (iM)

**Note:** Patients **CANNOT** opt out of being contacted for abnormal or clinically significant test results.

Patient **CAN** opt out of receiving health promotion and prevention reminders in any and all formats including SMS, letter and phone call.

---

# Considerations when sending commercial electronic messages (Direct Marketing)

When sending commercial electronic messages, the three key steps to follow are:

1. **Consent:** Only send commercial electronic messages with the addressee's consent - either express or inferred consent.\*
2. **Identify:** Include clear and accurate information about the person or business that is responsible for sending the commercial electronic message.
3. **Unsubscribe:** Ensure that a functional unsubscribe facility is included in all your commercial electronic messages. Deal with unsubscribe requests promptly.

\*Express consent is where a person has specifically requested messages from you and inferred consent is where there has been no direct request but it may be a reasonable expectation for the recipient to expect such messages.

---

# What is a Notifiable Data Breach (NDB)?

An eligible data breach arises when the following three criteria occur:

1. There is **unauthorised access** or unauthorised **disclosure** of personal information, or a **loss** of personal information that a practice holds
2. This is **likely to result in serious harm** to one or more individuals
3. The practice has **not been able to prevent the likely risk of serious harm with remedial action**





---

# Data breach examples

---

## Data breach instances may include:

- A database containing medical records is hacked (e.g. cyber-attack)
- Health information is mistakenly provided to the wrong person (e.g. test results being sent to the wrong patient)
- A device containing patients' medical records, such as a laptop or hard drive, is lost or stolen
- Inappropriate disclosure of health information to a family member or friend
- Viewing of health records by unauthorised practice staff members or contractors
- Inadequate steps to 'cleanse' or destroy information on computer hardware before it is disposed of
- Inadvertently placing health or other personal information on a publicly accessible website

---

# Accreditation and Privacy

## Indicators relating to Privacy

---

- ▶ **C6.3 A** Our patients are informed of how our practice manages confidentiality and their personal health information.
- ▶ **C6.3 B** Our patients are informed of how they can gain access to their health information we hold.
- ▶ **C6.3 C** In response to valid requests, our practice transfers relevant patient health information in a timely, authorised, and secure manner.
- ▶ **C6.3 D** Only authorised team members can access our patient health records, prescription pads, and other official documents

---

# Accreditation and Privacy

## Indicators relating to IT Security

---

- ▶ C6.4 A Our practice has a **team member who has primary responsibility** for the electronic systems and **computer security**.
- ▶ C6.4 B Our practice **does not store or temporarily leave the personal health information** of patients **where members of the public could see or access that information**.
- ▶ C6.4 C Our practice's **clinical software is accessible only via unique individual passwords that give access to information according to the person's level of authorisation**.
- ▶ C6.4 D Our practice has a **business continuity and information recovery plan**.



---

# Accreditation and Privacy

## Indicators relating to IT Security

---

- ▶ C6.4 E Our practice has appropriate procedures for the **storage, retention, and destruction of records.**
- ▶ C6.4 F Our practice has a **policy about the use of email.**
- ▶ C6.4 G Our practice has a **policy about the use of social media.**

---

# Insurance

Does your insurance protect against privacy/data breaches?

- Check with your insurance provided to make sure you are protected against unintentional privacy breaches.
- As well as cover for fines and penalties related to data breaches.




---

## Training Staff on Privacy


- Make it part of your staff induction process
- Ensure all staff signs a **Privacy & Confidentiality agreement**
- Have a **clear and transparent Privacy Policy** that all staff can understand and can easily & routinely offer to patients
- Include privacy **training refreshers** regularly as part of staff meetings
- Use team meetings to **discuss any slips or near misses** that could impact on patient Privacy. Make sure all staff feel supported to offer their ideas to improve practice processes.

# Sample staff training sheet & Privacy Policy template



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:

- Procedures
- Responsibilities
- 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](http://www.oaic.gov.au), or for privacy policies for GPs, visit [www.oaic.gov.au/privacy/privacy-resources/training-resources/privacy-policies-for-gps](http://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.

Privacy policy template for general practices v2

## [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 (e.g. staff training).

### What personal information do we collect?

The information we will collect about you includes your:

- Name, date of birth, addresses, contact details
- 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
- Identifiers
- 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 (eRx), My Health Record, e.g. via Shared Health Summary, Event Summary. You will need to specify if your practice participates in

# Thank you for participating!

---

Got a question?  
Email: [md@hotdoc.com.au](mailto:md@hotdoc.com.au)