Privacy & Confidentiality: A Guide for General Practice

June 2017

Magali De Castro
Clinical Director, HotDoc
Privacy & Confidentiality: A Guide for General Practice

This session will cover:

- Key privacy and confidentiality considerations for General Practice
- How to create robust policies and procedures to protect patient privacy
- Best tools and resources to support and train your team on the key privacy principles
What do we mean by Privacy & Confidentiality?

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
Upcoming training module: Developing your Privacy Policy
Presented by June Hannan
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 their processes regarding direct marketing
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
Accreditation and Privacy

Indicators relating to Privacy & Confidentiality

- Our practice uses three approved patient identifiers to correctly identify patients and their clinical information.

Correct patient identification is necessary when:

- a patient makes an appointment
- a patient presents to the practice for their appointment
- communicating with a patient over the telephone or electronically
- a patient phones asking for a repeat of a prescription
- collecting and managing information (e.g. scanned documents, x-rays)
Accreditation and Privacy

Indicators relating to Privacy & Confidentiality

- Our patients are informed of how our practice manages their confidentiality and personal health information.

- Only appropriate team members can access our patient health records.

- Our patients are informed of the processes we follow to provide them with access to their health information.
Accreditation and Privacy

Indicators relating to Privacy & Confidentiality

- In response to valid requests, our practice transfers relevant patient health information in a timely, authorised secure manner.

- Our practice transfers identified patient health information to a third party only after we receive informed patient consent.
Accreditation and Privacy

Indicators relating to Privacy & Confidentiality

- Our practice does not store or temporarily leave the personal health information of patients where members of the public could sight or access that information.

- Our practice’s computers are accessible only via individual passwords that give access to information according to the person’s level of authorisation.

- Our practice securely transfers electronic patient health information.
Accreditation and Privacy

Indicators relating to Privacy & Confidentiality

- Our practice has appropriate procedures for the storage, retention and destruction of records.

- Only authorised people can access prescription pads, letterhead, administrative records, and other official documents.

- Our practice has a policy on the use of email and social media.
  (New. 5th Edition Standards)
Considerations when sending commercial electronic messages (Direct Marketing)

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

This includes communication by:

- Email
- Short message service (SMS or text messages)
- Multimedia message service (MMS)
- Instant messaging (iM)
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.
Training Staff on Privacy & Confidentiality

- 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.
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.

The template covers:
- collecting personal information
- consent
- collection statement
- 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 review 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.aoic.gov.au, or for privacy policies for GPs, visit www.aoic.gov.au/primaryhealthcare/practiceprivacy-guidelines 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 procedures and legal requirements.

Privacy policy template for general practices

[Insert practice name] privacy policy

Current as at: [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. Our staff also need to see your personal information to 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 business for collecting, using, holding and sharing your personal information is to manage your health. We also collect information for other purposes, such as administrative and organizational needs (e.g., practice planning), work with the Commonwealth and other government agencies (e.g., Medicare), and business processes (e.g., staff training).

What personal information do we collect?

The information we will collect about you includes:
- names, date of birth, addresses, contact details
- history, 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
- 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 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.]
Upcoming training module: Developing your Privacy Policy

Presented by June Hannan
Thank you for participating!

Got a question?
Email: md@hotdoc.com.au