

SELECTED KEY POINTS FROM THIS PRIVACY POLICY

Please note that this is not an exhaustive summary. The full policy follows on page 2.



Information that is printed or handwritten on paper is stored in a secure cabinet which is accessible only to me.



For digital information, secure electronic systems, platforms, and software is used for storage (e.g., accounts, GP letters and supervision reports); processing (e.g., payments, Medicare claims and assessment questionnaires) and communication purposes (e.g., emails, efaxes, SMSs and telehealth).



I do not sell, share or trade your personal information. I do not provide your personal information to any organisations which conducts health research. I do not upload your personal information to any shared eHealth services such as *MyHealthRecord*.



Although I consult a cyber security strategist and take reasonable steps to ensure the security and safety of the “personal” and “sensitive” data I store, no data security or physical measures can guarantee 100% security of your data.



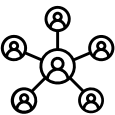
Digital communication methods such as email, SMS and eFax are not secure. While safeguards are in place to ensure your privacy, digital communication always presents a risk of data privacy issues.



With your consent and where it is required for the delivery of health or supervision services, personal information is shared with healthcare providers such your GP, psychiatrist, and third party funders such as Medicare; and for supervisees, with educational institutions, professional associations, employers, and other bodies related to your supervision.



I am obliged to share your personal information when it is required or authorised by law, or necessary to prevent a threat to your life, someone else’s life, or in the interest of public health or safety.



Once transmitted, I do not have control over your personal information such as Medicare letters to GPs or supervision reports to training institutions. After I have sent a letter, it may be forwarded to someone else, or uploaded to shared electronic eHealth services.



I am a sole practitioner and do not have administrative assistance. I am the only person managing your confidential communications, bookings, account, letters and file. In the event of incapacitation, a senior clinical psychologist will be legally granted access to inform patients and supervisees and close my practice.

Privacy Policy for Management of Personal Information

Introduction

I, Dr Wendy-Lynne Cooke, respect your privacy and right to control how your personal information is collected and used. "Personal information" refers to any information that may identify you, or by which your identity might reasonably be determined.

My practice adheres to the *Australian Privacy Principles* contained in the **Privacy Act 1988 (cth)**. This privacy policy for my practice provides you with information about how your personal information (including your mental health or clinical supervision information) is collected and used, and the circumstances in which I may share it with third parties. If I need to use your information for anything else, I will seek additional consent from you. In the event that unauthorised access, disclosure, or loss of your personal information occurs, I will endeavour to minimise the risk of consequential harm.

I am a sole practitioner and do not have an administrative assistant. I am the only person managing your file, bookings, and account. In the event of me becoming incapacitated to perform duties (e.g., due to death or illness), a senior clinical psychologist colleague will be legally granted access so that she can inform patients and carry out the necessary duties of the practice (such as closing files, writing to GPs, writing to Medicare, responding to subpoenas, and closing the practice).

Why and when your consent is necessary

When you register as a patient or supervisee of my practice, you provide consent for me to access and use your personal information so that I can provide you with the best possible mental health care or clinical supervision.

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

Your personal information is gathered and used for the purpose of providing psychological services (which includes assessing, diagnosing, and treating your presenting issue), or providing clinical supervision. Personal information is retained in order to document what happens during sessions and to enable me to provide a relevant and informed psychological or supervision service. I also use it for related business activities, such as Medicare claims and payments, practice audits, and business processes. Therefore, it may be necessary for me to disclose your personal information to third parties or contractors who are integral to the provision of my services.

What personal information do I collect?

The information I collect may include your:

- Names, date of birth, addresses, contact details, emergency contact details.
- Medical diagnosis of a mental health disorder as required for you to claim a Medicare rebate.
- Medicare number for identification and claiming purposes.
- "Sensitive" mental health information including medical reports, medications, referrals, health history, treatment history, social history, addictions history, family history, and risk factors.
- "Sensitive" clinical supervision information.
- Health fund details.
- Psychological assessments and session notes.
- Financial information (e.g., bank details or credit card information) if you have signed a request for me to automatically process your payments and/or your Medicare claims.
- Additionally, I may also collect any other information you provide when interacting with me.

How do I collect your personal information?

I may collect your personal information from when you initially contact me in person or electronically. This may include:

- Your personal and demographic information via your registration forms.
- During the course of providing psychological or supervision services, I may collect further personal information during your assessment, treatment or supervision sessions.

- During the course of providing psychological or supervision services, I may collect further personal information from other sources. This may include your GP, psychiatrist, allied health professionals, hospitals, your health fund, and Medicare.

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

I do not:

- Sell or trade your personal information to any third party.
- Upload any patient information to any shared eHealth services (e.g., My Health Record).
- Other than in the course of providing psychological or supervision services or as otherwise described in this policy, I will not share personal information with any third party without your consent.
- Share your personal information with anyone outside Australia without your consent unless such disclosure is otherwise required by law.
- Provide your data in any form (including de-identified) to any organisations which conduct research to improve population health outcomes.

I may use your personal information when:

- I provide you with information, updates, services or make you aware of new services available.
- I contact you through a variety of mediums, but not limited to email, SMS, telephone and by post.
- Other than in the course of providing psychological services or as otherwise described in this policy, I will not share personal information to third parties without your consent.
- I share personal information with third parties who work with me for business purposes, such as information technology providers, insurers, accountants, auditors, professional advisers, and lawyers – these third parties are required to comply with APPs and this policy.
- When it is required for the delivery of mental health services, information is provided to healthcare providers such as GPs, psychiatrists, other specialist medical practitioners, parents, employer, third-party funders such as Medicare and EAPs, and clinical supervisors of my work.
- When it is required for the delivery of clinical supervision services, information is provided to third parties such as training institutions or associations (e.g., evaluation reports).
- When I am required to write a report to another agency or professional, e.g., a GP or a lawyer.
- When I am required to disclose to another professional or agency (e.g., your GP) and disclosure of your personal information to that third party is for a purpose which is directly related to the primary purpose for which your personal information was collected.
- When it is required or authorised by law (e.g., court subpoenas, warrants, legal proceedings or in response to a request from a law enforcement agency).
- When it is necessary to lessen or prevent a serious threat to your life, health or safety; someone else's life, health or safety; 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 purposes of confidential dispute resolution processes.
- When there is a statutory requirement to share certain personal information (e.g., some diseases require mandatory notification).

What happens to information I send to other health professionals?

- I do not have control over information I am obliged to share with others such as GPs, psychiatrists, and allied health practitioners. For example, a GP may forward my Medicare letters to another health professional, or upload them a shared electronic eHealth service such as My Health Record.

How do I store and protect your personal information?

I am committed to ensuring that the information you provide to me is secure. I therefore consult a cyber security strategist for assistance with management of the data in my practice. I follow systems that aim to prevent unauthorized access or disclosure. These include physical, electronic and administrative procedures to safeguard and secure information and protect it from misuses, interference, loss, and unauthorised access, modifications, and disclosure.

Your personal information is stored at my practice in two forms, including hardcopy and digital formats.

- Information that is printed or handwritten on paper is stored in a secure cabinet which is accessible only to me.
- For digital information, secure electronic systems, platforms, and software is used for storage (e.g., accounts, GP letters and supervision reports); processing (e.g., payments, Medicare claims and assessment questionnaires) and communication purposes (e.g., emails, efaxes, SMSs and telehealth).

I take reasonable steps to ensure the security and safety of the systems I use and the data I store. I use 3rd party systems and services to provide my services to you. These 3rd party systems have their own security and safety protocols in place, however I am not able to directly affect, influence or assess their protocols. Unfortunately, no data security measures can always guarantee 100% security.

How secure is digital communication?

Digital communication methods such as email, SMS, andifax are not secure. There are inherent confidentiality risks. While safeguards are in place to ensure your privacy, digital communication always presents a risk of data privacy issues.

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

I encourage you to contact me to keep your personal information up to date. You have the right to request access to, and correction of, your personal information kept on file. By law, I may discuss the contents with you and/or give you a copy, subject to the exceptions in the Privacy Act 1988 (cth). If satisfied that the personal information is inaccurate, out of date or incomplete, reasonable steps will be taken in the circumstances to ensure that this information is corrected. All requests by patients for access to correction of personal information held about them should be lodged with me (Dr Wendy-Lynne Cooke) at admin@wendycooke.com.au. These requests will be responded to in writing within a reasonable time frame, and an appointment will be made if necessary for clarification purposes. An administration fee may be payable for the provision of information.

I reserve the right to refuse to provide you with information that I hold about you, in certain circumstances set out in the privacy act. For example, if required by law or where the information may be related to existing or anticipated legal proceedings, I may deny you request, setting out reasons for the refusal in writing.

How will a concern or complaint be handled at my practice?

I take complaints and concerns regarding privacy seriously. Upon request you can obtain a copy of the Australian Privacy Principles, which describe your rights and how personal information should be handled. You should express to me any privacy concerns you may have in writing. I will respond shortly after receiving written notice of your complaint and attempt to resolve the issue. Please send details of your complaint to me at PO Box 109, North Perth, WA 6906.

If you are not satisfied with my response, then you are entitled to lodge a formal complaint about the use of, disclosure of, or access to, your personal information. You may do so with the Office of the Australian Information Commissioner by phone on 1300 363 992, online at <http://www.oaic.gov.au/privacy/making-a-privacy-complaint> or by post to: Office of the Australian Information Commissioner, GPO Box 5218, Sydney, NSW, 2001.

Policy review statement

This policy will be reviewed regularly to ensure it is in accordance with any regulatory changes that may occur. It will be altered if necessary. I may modify this policy at any time at my sole discretion, and all modifications will be effective immediately.

Please note: If, after reading this form you are at all unclear about any of the information provided, please contact me prior to your appointment.