Gawler Surgical Specialists

Ph: 08 8523 2500 Fax: 08 8523 2400
reception@gawlersurgicalspecialists.com.au
16 Adelaide Road, Gawler South SA 5118

Contents

1. Introduction 2
2. Reference 2
3. What kinds of personal information do we collect ? 2
4. How do we collect and hold personal information ? 3
5. Why do we collect, hold, use and disclose personal information ? 3
6. Email, SMS and digital communication 4
7. Patient consent 5
8. Use of AI 5
9. Practice procedure 6
10. Staff responsibility 7
11. Anonymity and pseudonyms 7
12. Overseas disclosure 7
13. How can you access and correct your personal information? 7
14. Privacy-related questions and complaints 8
15. Contact details for privacy related issues 8
16. Updates to this Policy 8
17. Document Information: 8

1. Introduction

Our practice is committed to best practice in relation to the management of information we collect.

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 complaints;
- whether we are likely to disclose personal information to overseas recipients

This policy will guide Practice staff in meeting their legal obligations. It also provides details to patients how the Practice uses their personal information.

2. Reference

This Practice is bound by the Federal Privacy Act 1998 ('the Privacy Act') and National Privacy Principles. 'Personal health information' (PHI) is a subset of personal information and can include any information collected to provide a health service.

This information includes medical details, family information, name, address, employment, demographic data, past medical and social history, current health issues, future medical care, Medicare number, account details and any health information such as a medical opinion about a person's health, disability or health status.

It includes the formal medical record, whether written or electronic, and information held or recorded on any other medium such as letters, faxes and information conveyed verbally.

Office of the Australian Information Commissioner issues a set of guidelines ("Australian Privacy Principles (APP) Guidelines").

The APP provides a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APP consists of 13 principle-based laws and applies equally to paper-based and digital environments. The APP complements the long-standing general practice obligation to manage personal information in a regulated, open and transparent manner.

3. What kinds of personal information do we collect ?

The type of information we collect, and hold includes:

- Your name, address, date of birth, email, employment details and contact details,
- Medicare number, DVA number and other government identifiers, medical insurance details, Workcover Claim details, etc. (as applicable),

Other health information about you, including

- notes of your symptoms or diagnosis and the treatment given to you
- your referrals from your GPs or other treating practitioners
- your specialist reports and test results
- your appointment and billing details
- your prescriptions and other pharmaceutical purchases
- your healthcare identifiers
- Any other information about your race, sexuality or religion, when collected by a health service provider

4. 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 centers, specialists, hospitals, the My Health Record system, electronic prescription services, Medicare, your health insurer, the Pharmaceutical Benefits Scheme

We hold your personal information in various formats and various locations. This may include one or more of the following:

- Holding your information on an encrypted database (currently Medical Wizard)
  (This may change without notice to you based on requirements of the organization)
- Holding your information in hard copy format;
- Holding your information in secure cloud storage: The information on cloud storage relates to (but not limited to) fax and email communications with other providers in relation to providing you with appropriate healthcare;

There may be instances where such information (cloud stored information, database to keep track of patients and due treatment) is shared with GSS for managing your health but is not exclusively or primarily controlled by GSS. In such instances, GSS and its staff will try our best to ensure that all data owners comply with applicable Australian laws but are not able to accept any liability for security / confidentiality of such information.

5. 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;

- 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 (including debt collection agencies), management of our IT systems;
- to and during communication with other doctors and allied health professional involved in your healthcare;
- to obtain, analyze and discuss test results from diagnostic and pathology laboratories;
- for identification and insurance claiming;
- transfer of healthcare records and communications to other participating members of your healthcare team, including secure electronic communication methods (like, but not limited to, Argus, Fax, etc) and Australia Post letters;
- 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
- For communications with other doctors and allied health professionals, we may transmit this information as a document attached to emails. When doing so we will take reasonable care to avoid sending these emails to incorrect recipients and will endeavor our best to protect such documents with passwords (which will be communicated to the concerned parties by a separate mode of communication like SMS, in person or fax) to comply with relevant Australian Privacy Regulations. However, at times, such information may need to be transmitted un-encrypted due to technical limitations beyond our control

Exceptions (need to disclose information without prior patient consent) to above include:

- As required by law
- 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 establish, exercise or defend an equitable claim or a dispute resolution process.

6. Email, SMS and digital communication

We understand that electronic communication offers convenience, and we strive to facilitate this while upholding the highest standards of privacy and security.

Our practice offers electronic communication methods, including email and SMS, to enhance patient convenience and facilitate timely exchange of information. These methods are primarily used for non-urgent matters such as: **Appointment reminders and confirmations, Result updates, Recalls and follow-ups**.

Your consent is paramount for all electronic communications.

- **Implied Consent:** Consent may be implied when you initiate electronic communication with the practice or provide your email address or mobile number for communication purposes. For instance, if you provide your contact details during registration, it is generally reasonable to imply consent for communications directly related to your ongoing care, such as appointment reminders or notifications of test results that require follow-up.

- **Express Consent:** For communications that are not directly related to your immediate healthcare or for direct marketing purposes, express consent will be sought. This may involve ticking a consent box on a registration form or providing verbal consent which is then documented in your clinical record

- You have the right to withdraw your consent at any time

While we take reasonable steps to protect your privacy, it is important to understand the inherent risks associated with electronic communication:

- **Unencrypted Communication:** Standard email is generally not a secure form of communication, and we cannot guarantee the security or confidentiality of information transmitted via unencrypted email. There is a risk that emails and/or attachments could be intercepted, read, or forwarded by unintended recipients.

- **Sensitive Information:** We generally refrain from sending confidential or sensitive patient information, such as detailed test results or new diagnoses, via unencrypted email. Such information typically requires a face-to-face consultation or a telehealth appointment with your doctor.

Secure Messaging: Where possible and appropriate, we utilize secure messaging facilities (e.g., Healthlink, Medical Objects) for communication with other healthcare providers. For sensitive information sent to patients via email, we may use password protection or other encryption methods, and the password will be provided through a separate, secure channel (e.g., SMS or phone call).

7. Patient consent

The Practice will only interpret and apply a patient's consent for the primary purpose for which it was provided. The Practice staff must seek additional consent from the patient if the personal information collected may be used for any other purpose.

8. Use of AI

We may use an AI medical scribe, (currently Heidi but subject to change without notice), to assist with documentation. This technology is designed to listen to the conversation during your consultation and generate a draft clinical note, referral letters, or other relevant documents. The primary purpose of using Heidi is to allow our practitioners to focus more attentively on you, the patient, rather than on manual note-taking, thereby enhancing the quality of your consultation and reducing administrative burden.

Your participation is entirely voluntary, and you can change your decision at any time, even after the consultation begins.

Data Collection and Processing: Heidi processes audio data from your consultation to produce a summary of the information. It is important to note that Heidi does not store audio recordings; instead, it securely transcribes the audio into text in real-time. This text is then used to generate the clinical documentation. Heidi employs pseudonymisation techniques, replacing personal names with anonymous equivalents, and patient identifiers are stored separately from de-identified transcripts in siloed databases to enhance security. All patient data is encrypted both during transmission and while stored, using advanced encryption standards to

ensure confidentiality and integrity.

Data Storage and Security: For Australian users, all consultation data and AI processing occur on secure cloud servers located within Australia. Heidi Health ensures that data is stored in compliance with Australian Privacy Principles (APP) and is protected according to ISO 27001 and SOC 2 Type II requirements, which are recognized international standards for information security management. **Heidi does not use patient data to train its models, nor does it sell user data to third parties.** The company maintains non-retention policies, meaning that while transcripts and notes are stored, audio is never retained, and users have control over data deletion schedules.

Patient Consent: Your **informed consent is paramount** to our use of AI scribes. Before each consultation where Heidi is used, we will seek your verbal confirmation of consent. This consent will be documented in your clinical record. We will explain how Heidi works, what information it collects, and how that information will be used. This transparency is crucial for building and maintaining your trust. You have the right to decline the use of the AI scribe at any time, and your decision will not affect the quality of care you receive. If you do not consent, the consultation will proceed without the use of the AI scribe.

Accuracy and Practitioner Responsibility: While Heidi is designed for accuracy, the AI-generated notes are considered draft documents. Our healthcare practitioners are responsible for reviewing and editing all AI-generated documentation for accuracy and completeness before it is finalized and added to your medical record. This includes verifying factual correctness, incorporating non-verbal cues, and ensuring all clinically relevant information is captured. The ultimate responsibility for the accuracy of your medical record rests with the treating clinician.

You have the right to decline the use of the AI scribe at any time, and your care will remain unaffected; your clinician will simply take notes manually instead. If you wish to opt out, please inform our reception team when booking your appointment or let your clinician know at the beginning of your consultation.

9. Practice procedure

We take reasonable steps to protect information held from misuse and loss and from unauthorized access, modification or disclosure.

Our staff are trained and required to respect & protect your privacy and adhere to strict standards in dealing with your personal information in accordance with relevant legal provisions. All hard copies containing your personal information are destroyed by secure confidential paper destruction methods.

The Practice will:

- Provide a copy of this policy upon request
- Ensure staff comply with the APP and deal appropriately with inquiries or concerns
- Take such steps as are reasonable in the circumstances to implement practices, procedures, and systems to ensure compliance with the APP and deal with inquiries or complaints
- Collect personal information for the primary purpose of managing a patient's healthcare and for financial claims and payments.

10. Staff responsibility

The Practice's staff will take reasonable steps to ensure patients understand:

- What information has been and is being collected
- Why this information is being collected
- Whether there is a legal requirement
- How the information will be used or disclosed
- Why and when your consent is necessary & needed

The Practice's staff will also endeavor to explain and assist patients with

- Procedures for access and correction of information, and
- Responding to complaints of information breaches, including by providing this policy

11. Anonymity and pseudonyms

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

In our practice, we will not be able to deal with or provide care to individuals who do not wish to provide us with all the required identifiers.

12. Overseas disclosure

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)
- overseas transcription services to transcribe clinical notes or letters in relation to your care
- overseas based cloud storage (for secure storage and access; no personal information is divulged to the cloud service provider). We do make efforts to use services of providers where the information is stored and remains within the geographical boundaries of Australia.
    - Where your information is stored on overseas based cloud storage, it will be in folders which are password protected. [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 authorize us to disclose it

13. How can you access and correct your personal information?

You have a right to seek access to, and request correction of the personal information which we hold about you. There may be a fee associated with this access and depends on the nature and quantum of the information

access requested. It will be detailed to you when you request this information.

For details on how to access and correct your health record, please contact us and submit your request in writing. We will normally respond to your request within 30 working days.

14. 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 (details below):

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

15. Contact details for privacy related issues

We may require proof of your identity if you wish to access or modify your personal details that we have on our records.

To view or update your personal details, or if you have questions, please contact the secretary or practice manager at the contact details mentioned in the letter head

16. 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. An updated copy of this policy is available on request and will be published on the practice's website.

17. Document Information:

Version:	4.0
Date of first approval:	16-Jan-19
Date of revision:	08-Aug-25
Revision due in:	36 months