HSFP Privacy Policy

Address	Level 3/11 High Street Launceston Tasmania 7250
Telephone	03 6334 5500
Email	reception@hsfp7.com.au

1. Our commitment to privacy

High Street Family Practice is committed to protecting the privacy, confidentiality and security of the personal and health information entrusted to us.

We manage personal information in accordance with:

- the Privacy Act 1988
- the Australian Privacy Principles
- applicable state/territory privacy and health records legislation
- the My Health Records Act 2012, where applicable
- professional, ethical and legal obligations applying to healthcare providers
- the current RACGP Standards for general practices.

This policy explains how we collect, hold, use, disclose and protect personal information. It also explains how patients can access or correct their information, raise a privacy concern and make choices about how their information is handled.

This policy applies to all members of the practice team, including GPs, nurses, allied health professionals, administrative staff, contractors, students and others who may have authorised access to information held by the practice.

2. What is a patient health record?

A patient health record is the collection of health and related personal information held by the practice about an individual patient.

It may include information created by our practice team and information received from other healthcare providers or authorised sources.

Patient health records may be held electronically, on paper or in another format. They may include:

- name, date of birth, address and contact details
- Medicare or other healthcare identifiers
- emergency contact, next of kin, carer or guardian details
- cultural, language and communication needs

- consultation notes, medical history and current health information
- diagnoses, medicines, allergies and adverse reactions
- test results, referrals, reports and correspondence
- family, social or lifestyle information relevant to care
- care plans, recalls and reminders
- clinical photographs, images or recordings
- consent, appointment, billing and payment records
- communication records, feedback and complaints
- information prepared using approved digital or artificial intelligence tools.

The patient health record held by this practice is separate from the national My Health Record system.

We aim to collect information directly from the patient wherever practical.

We may also receive information from another healthcare provider, hospital, diagnostic service, pharmacy, carer, government agency or another authorised source.

3. How we inform patients about collection

When we collect personal information, we take reasonable steps to explain:

- why the information is being collected
- how it may be used or disclosed
- whether providing it is required or optional
- what may happen if it is not provided
- how to access this policy.

This information may be provided through a registration form, privacy collection notice, consent form, website, online booking system or during a discussion with the practice team.

4. How we use patient information

We use patient information primarily to provide, coordinate and manage healthcare.

We may also use it to:

- manage appointments and patient communications
- arrange referrals, prescriptions and investigations
- provide recalls, reminders and preventative healthcare
- process Medicare, insurance or other payments
- manage complaints and incidents
- meet legal, regulatory and professional obligations
- support accreditation, quality improvement and service planning

- undertake approved research or data activities where legal requirements are met.

We only use or disclose information for the purpose for which it was collected or for another purpose that is permitted by law.

Where clinical software or another approved system uses document automation to prepare a referral letter, the referring practitioner reviews the letter before it is sent and removes information that is not relevant to the referral. Only medical information relevant to the purpose of the referral is included.

5. Sharing patient information

We may share relevant information with people or organisations involved in a patient's care, including:

- GPs and other healthcare providers
- hospitals and health services
- pathology and imaging services
- pharmacies and allied health providers
- My Health Record
- Medicare and other government programs
- contractors who provide authorised services to the practice.

Information may also be disclosed when:

- the patient has consented
- disclosure is required or authorised by law
- it is necessary to prevent or lessen a serious threat to health or safety
- a valid court order, subpoena or other legal authority applies.

We provide only the information reasonably necessary for the purpose.

We do not assume that family members, partners or carers are automatically entitled to receive a patient's health information.

6. Consent and patient choices

We seek consent where it is required or appropriate.

This may include consent for:

- sharing information outside the usual provision of healthcare
- communicating through email or another method that carries privacy risks
- making clinical photographs or making, duplicating or storing real-time audio or visual recordings of consultations, including telehealth and other remotely conducted consultations
- using an optional AI-assisted documentation tool

- using identifiable information for research, teaching or promotional purposes.

Consent may be withdrawn for future uses or disclosures.

Patients may ask to interact with us anonymously or by using a pseudonym. We will allow this where it is lawful and practical. It may not be possible where accurate identification is needed for safe care, Medicare claims, prescriptions, referrals or legal requirements.

7. Email, SMS, telehealth and online services

We may communicate with patients through telephone, SMS, email, secure messaging, patient portals, telehealth platforms or online booking systems.

Electronic communication can involve risks including messages being accessed by another person, sent to the wrong recipient or stored outside the practice.

We take reasonable steps to use appropriate and secure communication methods. Patients should keep their contact details current and tell us about their communication preferences.

Email, SMS and online messages should not be used for emergencies or urgent clinical matters unless the practice has specifically advised otherwise.

8. Artificial intelligence and digital tools

The practice may use approved digital or artificial intelligence tools to support clinical documentation, communication, administration or decision support.

Before using a tool that handles patient information, the practice considers its privacy, security, data storage, access and retention arrangements.

We do not enter identifiable patient information into publicly available or unapproved AI tools.

Patients will be told when an AI-assisted documentation tool is being used. If the tool makes, duplicates or stores a real-time audio or visual recording of a consultation, including a telehealth or other remotely conducted consultation, it will not be used unless the patient has first given consent.

AI does not replace professional judgement or clinical responsibility. Information produced by an AI tool must be carefully reviewed for accuracy, particularly where generated information will become part of a patient health record.

9. Website information, cookies and tracking

Our website or online services may collect basic technical information such as device type, browser type, pages visited and the date and time of access.

The practice may use essential cookies or approved analytics tools to operate and improve its website.

We do not knowingly use website tracking technologies to collect sensitive health information for advertising without the consent and safeguards required by law.

10. Storage, security and overseas access

Patient information may be held in clinical software, secure electronic systems, paper records, cloud services or approved third-party systems.

We take reasonable steps to protect information from loss, misuse, interference, unauthorised access, modification or disclosure. These measures include access controls, secure passwords, staff confidentiality requirements, backups and secure disposal.

Practice team members may only access patient information when it is required for their work.

11. Accessing and correcting information

Patients may request access to the personal information we hold about them.

Access may be provided as a copy, by inspection or through another agreed method. We will verify the person's identity before releasing information.

Access may be refused or limited where permitted by law, including where it could create a serious threat to health or safety or unreasonably affect another person's privacy.

Patients may also ask us to correct information they believe is inaccurate, incomplete, out of date, irrelevant or misleading.

Corrections to clinical records are made in a way that preserves the original record and maintains its integrity.

A reasonable fee may apply for the cost of providing access

Requests should be directed to:

Privacy contact: Olivia - Practice Manager
Email: manager@hsfp7.com.au
Postal address: Level 3/11 High Street Launceston TAS 7250

We aim to respond within 30 days or within another timeframe required by applicable legislation.

12. Privacy incidents

The practice investigates suspected privacy incidents and takes steps to contain and manage any risk.

Where a data breach is likely to cause serious harm, affected individuals and the Office of the Australian Information Commissioner will be notified where required by law.

13. Privacy concerns and complaints

Patients may contact us if they have questions or concerns about how their information has been handled.

Complaints can be made verbally or in writing to:

Privacy contact: Olivia
Telephone: 03 6334 5500
Email: manager@hsfp7.com.au
Postal address: Level 3/11 high Street Launceston TAS 7250

We will acknowledge the concern, investigate it and explain the outcome and any action taken.

Making a privacy complaint will not affect a patient's access to healthcare.

A patient who is not satisfied with our response may contact the Office of the Australian Information Commissioner or the relevant state or territory privacy or health complaints body.

14. Availability and review

This policy is available:

- on our website at www.highstreetfamilypractice.com.au
- from reception
- in another format on request.

Review Date, current as of: November 2026

We review this policy regularly and when laws, accreditation requirements, services or information-handling practices change.