

Privacy Policy

Case Conference Connect and HMR Connect (formerly HMR Tracker) are digital platforms developed, owned, and managed by Simple Care Connect Pty Ltd ACN 699 124 448 (**Simple Care Connect, we, us or our**). We are committed to maintaining the highest standards of privacy, security, and compliance in all aspects of our service delivery. Simple Care Connect oversees all operational, technical, and administrative aspects of Case Conference Connect and HMR Connect to ensure the platforms align with healthcare industry best practices and regulatory requirements.

Your privacy is important to us

This privacy policy explains how Simple Care Connect collects, holds, uses and discloses personal information, in accordance with the Australian Privacy Principles and the Privacy Act 1988 (Cth) (**Privacy Act**).

In this policy, “Simple Care Connect” includes all websites, applications, case conferencing tools, and services provided by us.

Types of Personal Information We Collect

We may collect and hold the following types of personal information: - Names, addresses, email addresses, and phone numbers; - Payment details (such as credit or debit card information); - Information on your location and device usage; - Information you provide when accessing our applications or websites; - Details of services you use or request from us; - If you are a patient, we may collect your Medicare or Department of Veterans Affairs number and sensitive health-related information relevant to your care.

We take particular care when handling sensitive health information, which is only collected with your consent or where permitted by law.

How We Collect Personal Information

We may collect personal information directly through: - Online forms and registrations; - Communications such as emails, phone calls, and meetings; - Information submitted by health professionals on behalf of their patients; - Use of our platforms, including data entered during case conferencing or health management.

Patients may opt out of having their personal information shared by notifying their healthcare provider.

Purpose of Collecting Your Personal Information

We may collect and use your information to: - Provide you with secure access to Simple Care Connect and related services; - Facilitate communication between you and your health professionals; - Support digital case conferencing for collaborative care planning; - Respond to enquiries and customer service requests; - Provide updates and

marketing materials (unless opted out); - Manage payments, internal administration, and compliance; - Fulfil our legal and professional obligations.

If we are unable to collect necessary personal information, we may not be able to provide services to you.

Sharing Health Information in Case Conferencing

Our digital case conferencing tool allows authorised health professionals to securely share and view patient information. Information is shared only with team members directly involved in a patient's care. Access is restricted to authorised users and governed by confidentiality and ethical obligations.

A patient's General Practitioner will seek the patient's consent to share patient information via the digital case conferencing tool.

Disclosure of Personal Information

We may disclose your personal information to: - Health professionals involved in your care; - Entities involved in resolving complaints or disputes; - Professional advisers or legal authorities, where permitted or required by law; - Other third parties, with your consent.

We may disclose your personal information to overseas recipients, including our offshore resources and third-party service providers, in accordance with the "Third-Party Providers and Offshore Disclosures" section of this policy. Except as outlined in this policy, or under exceptional circumstances permitted by law, we will not share your personal information with anyone outside Australia without your consent.

How We Store and Protect Personal Information

Personal information is primarily held securely in electronic formats on secure servers located within Australia. We maintain safeguards to prevent misuse, unauthorised access, or disclosure, and ensure information is protected against loss or interference. However, as detailed in the "Third-Party Providers and Offshore Disclosures" section below, some information may be stored, processed, or accessed by authorised providers and personnel located outside Australia.

Third-Party Providers and Offshore Disclosure

We may utilise outsourced service providers and cloud computing service providers, including:

- Binary Lane, for Australian-based server hosting and data storage;
- Twilio, for live video conferencing and automated transcription. Audio and video files are not recorded or retained;

- Simple Healthcare Solutions Pty Ltd, for administrative, onboarding and operational support;
- Cloudflare, for website and application security; and
- selected CRM, communications, payment-processing and IT support providers, where required to operate and support our services.
- and other third parties from time to time and as separately notified to you.

In providing our services, we use a range of third-party software platforms, cloud services, document management systems, user portals, payment providers, reporting tools, offshore resources based in the Philippines, and supporting IT/security services. These systems may collect, store, process, transmit, protect, back up, or provide access to personal, health, and user information where required for the delivery of our services, administration of our business, communication with users, document management, payment processing, regulatory compliance, and cyber security.

Some providers may store or process information outside Australia, or may allow authorised support, operational, or security personnel located outside Australia to access information. We take reasonable steps to select and use reputable providers and apply appropriate controls where available, such as multi-factor authentication, access controls, role-based permissions, encryption, audit logging, monitoring, backup, and incident response processes.

Each third-party provider remains responsible for the operation, availability, security, and privacy practices of its own platform. Further information about each provider's handling of data should be reviewed in that provider's privacy policy, security documentation, data processing terms, or terms of service.

Data Retention

We retain personal and health information only for as long as needed to meet legal, regulatory, and clinical requirements. Information no longer required is securely deleted or de-identified.

Data Security Breaches

We have established procedures to identify, assess, and manage potential data security breaches. In the event of a data breach that is likely to result in serious harm to individuals whose personal or sensitive health information has been compromised, we will promptly notify the affected individuals and the relevant supervisory authority in accordance with our legal obligations. We will also take immediate steps to contain the breach, investigate its cause, and mitigate any potential harm.

Your Privacy Rights

Under the Privacy Act, you have the right to:

- Access the personal information we hold about you;
- Request correction or updates to your information;
- Withdraw your consent at any time;
- Make a privacy-related complaint.

Accessing or Correcting Your Information

To access or correct your personal information, please contact us in writing using the details below. We may verify your identity before actioning your request. If access is restricted for privacy or legal reasons, we will explain why.

Direct Marketing

We may use your personal information to send relevant marketing materials. You may opt out at any time by contacting us.

Cookies and Website Usage

Our websites use cookies to: - Manage sessions; - Enhance security; - Analyse usage trends and improve user experience.

You can manage cookie settings via your browser. Blocking cookies may limit access to some site features.

Anonymity and Pseudonyms

You may choose to remain anonymous or use a pseudonym when contacting us, unless it is impractical or unlawful for us to respond without identifying you.

Making a Privacy Complaint

If you believe we have breached your privacy rights, please contact us in writing. We will endeavour to respond within 30 days. If you are not satisfied, you may contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

Updates to This Privacy Policy

This policy may be updated to reflect changes to our services, technology, or legal obligations. We encourage you to review it periodically.

Contact Us

If you have any questions about this privacy policy, wish to access or correct your personal information, or want to make a privacy-related complaint, please contact our Privacy Officer at:

- **Email:** mitch.fox@simplecareconnect.com.au
- **Postal Address:** 2/81 Grange Road, Welland, 5007, South Australia