
SW HEALTH PRIVACY POLICY

Effective: 7 September 2026

Approved by: Matthew Holt, Managing Director

1. Purpose

Safework Health (SW Health) protects personal and health information under the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), applicable state and territory laws, and the Privacy and Other Legislation Amendment Act 2024. This policy explains how we collect, hold, use, disclose and secure information, and uphold individual privacy rights.

2. Scope

This policy applies to all SW Health employees, contractors and representatives, and to personal and health information handled through drug and alcohol testing, biological health surveillance, occupational health, employment processes, digital platforms and third-party providers.

3. Definitions

- **Personal information:** Information or an opinion about an identified or reasonably identifiable person, whether accurate or recorded.
 - **Health information:** Personal information about health, medical history or health services.
 - **APPs:** Privacy Act principles governing personal information.
 - **Cross-border disclosure:** Disclosure of personal information to an overseas recipient.
 - **Sensitive information:** Information such as health or biometric data, as defined by the Privacy Act.
 - **Notifiable data breach:** An eligible breach under Part IIIC of the Privacy Act requiring notification to affected individuals and the OAIC.
 - **Automated decision-making (ADM):** Computer-assisted action substantially and directly related to a decision that may significantly affect a person's rights or interests; amended APP 1 requirements apply from 10 December 2026.
-

4. Our Commitment and Objectives

SW Health will:

- Collect only information needed to provide services or meet legal obligations.
 - Permit anonymous or pseudonymous dealings where lawful and practicable.
 - Secure information against misuse, loss and unauthorised access, modification or disclosure.
 - Provide access and correction rights, subject to legal exceptions.
 - Comply with privacy laws and applicable standards.
 - Assess and respond to breaches under the Notifiable Data Breaches scheme.
-

4.1 Why We Collect Personal Information

We collect personal and health information to:

- Provide suitable services, advice and communications.
- Improve, administer and evaluate services.
- Manage charges, billing and debt recovery.

- Meet legal and regulatory obligations.
- Support privacy-protected, data-driven service improvement.

4.2 Types of Information Collected

- **Drug and alcohol testing and biological health surveillance:** name, date of birth, occupation, postal and email address, telephone number, current medication, consented biometric data where relevant, and other necessary information.
- **Occupational health services:** the above information plus health history, medical records and consented health-risk assessment data where applicable.
- **Employment applications:** work history, skills, tax, superannuation and banking details, employee health, current medication and vaccination records, references, lawful background checks, and other relevant information.

4.3 How We Collect Information

Where practicable, we collect information directly through consent and chain-of-custody forms, discussions, telephone or secure digital platforms. We may collect it from authorised representatives or previous health professionals with consent or where law permits. Third-party collection must be transparent and APP-compliant. Sensitive health information is collected only with consent or under a lawful exception.

4.4 Use and Disclosure of Information

We use or disclose information only as authorised, including for:

- Service management, funding, monitoring, planning, evaluation and complaints.
- Legal, regulatory, accreditation, quality assurance and clinical audit requirements.
- Billing, debt recovery, subpoenas and legal proceedings.
- Insurance claims submission.
- Directly related health-service activities reasonably expected by the individual.
- Permitted research using de-identified data.

We disclose information overseas only in accordance with APP 8, including where the recipient is subject to comparable privacy protections or contractual safeguards provide equivalent protection.

4.5 Storage and Security

We store information in paper and electronic form and protect it through:

- Staff confidentiality and secure document storage.
- Controlled system access, encryption and multi-factor authentication where applicable.
- Private settings for confidential discussions and identity checks before access.
- Lawful retention and secure destruction.
- Technical and organisational controls proportionate to information sensitivity.

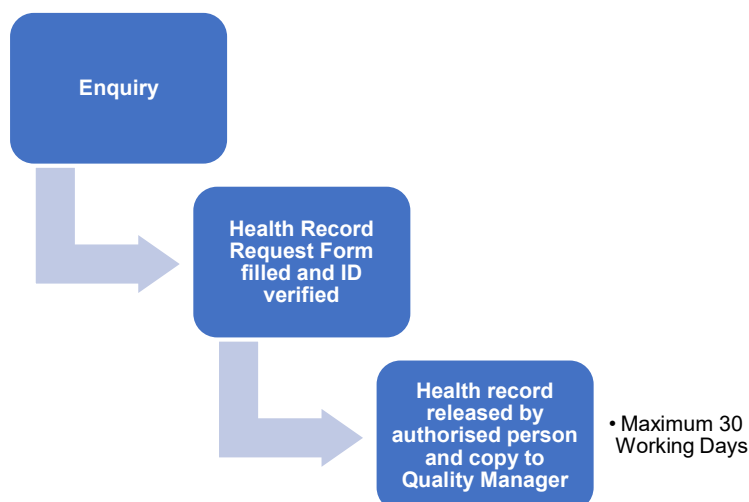
4.6 Access to Personal Information

SW Health owns the medical records it creates; customers may own reports supplied under service agreements. Regardless of ownership, individuals may access personal and health information held about them, subject to lawful exceptions.

Request access at info@swhealth.com.au or a pre-employment medical centre. We verify identity and respond within a reasonable period, usually no more than 30 calendar days. We do not charge for making a request; however, a reasonable, non-excessive fee may apply for providing access and must be paid before the records are released.

1. Submit the Health Record Request Form and evidence of identity.
2. Pay any applicable access fee.
3. An authorised person releases the record and sends a copy to the Quality Manager.

4. Access is provided within the applicable response period.



4.7 Correction of Personal Information

Individuals may request correction of inaccurate, out-of-date, incomplete, irrelevant or misleading information through the access-request channels. We will take reasonable steps to correct it or provide written reasons for refusal and available complaint options.

4.8 Online Privacy

SW Health protects online privacy by:

- Allowing anonymous website visits where no personal information is collected.
- Using email addresses only for requested services or responses, unless consent or law authorises otherwise.
- Sharing only aggregate, non-identifiable website statistics.
- Using secure transmission, security audits and disclosed tracking technologies with required consent.
- Advising users that linked third-party sites have separate privacy practices.

4.9 Complaints

Direct privacy concerns to the Quality Manager. If unresolved, contact SW Health Head Office on 1300 795 227. Allow us a reasonable opportunity, generally 30 days, to respond before external escalation.

Individuals may also complain to the [Office of the Australian Information Commissioner](https://www.oaic.gov.au): 1300 363 992, enquiries@oaic.gov.au, or GPO Box 5288, Sydney NSW 2001.

4.10 Data Breach Notification

SW Health identifies, contains, assesses and responds to data breaches. If unauthorised access, disclosure or loss is likely to cause serious harm and remedial action has not removed that risk, we will notify affected individuals and the OAIC as soon as practicable under Part IIIC of the Privacy Act. Staff must immediately report suspected or actual breaches to the Managing Director.

4.11 Automated Decision Making

Automated systems assist with laboratory drug-screen classifications and sample-integrity checks, and with clinic outputs such as spirometry grades, ECG interpretation, audiometry flags and hearing-protector fit ratings. Instant immunoassay screens are preliminary; not-negative results require laboratory confirmation.

A qualified scientist reviews every laboratory result, and a competent clinician reviews clinic output. An Occupational Physician, Examining Medical Officer or Authorised Medical Adviser signs applicable medicals. These systems support testing and reporting but do not decide fitness for duty, employment, site access or regulatory authorisation; the requesting organisation decides using a human-signed report. Queensland mining medical results may be uploaded to ResHealth, while SW Health remains responsible for submitted traces and physician sign-off. Individuals may dispute laboratory results under the Test Result Dispute Resolution Procedure, including referee-sample analysis, or request review and retesting of clinic findings.

5. Implementation and Responsibilities

5.1 Management Responsibilities

- Ensure compliance with all the APPs and applicable state and territory privacy and health-privacy laws.
- Oversee secure information handling, staff training and complaint resolution.
- Maintain this policy and test breach-response procedures as laws, operations and standards change.

5.2 Employee Responsibilities

- Follow this policy, protect confidentiality and comply with security controls.
 - Collect, use and disclose information only as authorised.
 - Immediately report suspected breaches to the Quality Manager.
 - Complete required training and remain informed of policy updates.
-

6. Forms and References

- [GEN - FRM - 2150 - SWG – Health Record Request Form](#)
 - [OCH - FRM - 26131 - SWHOCCH - Health Record Request Form - Occupational Division](#)
 - [QUA - SOP - 2810 - SWQ - Data Breach Notification Procedure](#)
-

7. Commitment Statement

SW Health protects privacy while delivering high-quality services. We handle personal and health information lawfully, securely and transparently, using contemporary controls and clear processes. Individuals may contact us with questions or concerns about our privacy practices.

Signed:



Matthew Holt
Managing Director
7 September 2026