SW HEALTH PRIVACY POLICY
Effective Date: 26 August 2025
Approved by: Matthew Holt, Managing Director

1. Purpose

Safework Health (SW Health) is committed to protecting the privacy and personal information of individuals in accordance with the Australian Privacy Principles under the Privacy Act 1988 (Cth) and applicable state and territory privacy laws. This policy outlines how we collect, manage, use, disclose, and protect personal and health information to ensure compliance with legal obligations and respect for individual privacy rights. *It also reflects our commitment to adopting contemporary data protection practices in response to evolving digital and regulatory landscapes.*

2. Scope

This policy applies to all employees, contractors, and representatives of SW Health, as well as all personal and health information collected, held, or processed by SW Health while providing services, including drug and alcohol testing, biological health surveillance, occupational health services, and employment-related processes. *It extends to data processed through digital platforms and third-party service providers.*

3. Definitions

- **Personal Information**: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not.
- **Health Information**: A subset of personal information concerning an individual's health, medical history, or health services provided to them.
- **Australian Privacy Principles (APPs)**: Principles set out in the Privacy Act 1988 (Cth) that regulate the handling of personal information.
- **Transborder Data Flows**: The transfer of personal information to entities outside the state, territory, or country in which the individual resides.
- ***Sensitive Information*****:** *Information including health or biometric data, as defined under the Privacy Act 1988 (Cth).*

4. Our Commitment and Objectives

SW Health is dedicated to safeguarding the privacy of individuals by:

- Collecting personal and health information only where necessary for providing services or meeting legal obligations.
- Allowing individuals to interact with us anonymously or *pseudonymously* where lawful and practicable (e.g., general inquiries about services).

- Ensuring personal and health information is stored securely and protected from misuse, loss, or unauthorised access, modification, or disclosure.
- Providing individuals with access to their personal and health information, subject to legal exceptions, and addressing privacy concerns promptly.
- Complying with all relevant privacy laws, including the Australian Privacy Principles, state/territory regulations, *and emerging data protection standards*.

4.1 Why We Collect Personal Information

We collect personal and health information to:

- Understand individuals' needs to provide appropriate services and advice.
- Communicate with individuals regarding service delivery.
- Improve the quality of our services.
- Administer and manage services, including charging, billing, and debt collection.
- Comply with legal and regulatory requirements.
- *Support data-driven improvements to service delivery while ensuring privacy protections.*

4.2 Types of Information Collected

For **Drug and Alcohol Testing** and **Biological Health Surveillance**, we may collect:

- Name
- Date of birth
- Occupation
- Address (postal and email)
- Telephone numbers
- Current medication
- *Biometric data (where relevant and consented)*
- Other information necessary for our functions and activities.

For **Occupational Health Services**, we may collect:

- Name
- Date of birth
- Occupation
- Address (postal and email)
- Telephone numbers
- Current medication, health history, and medical records
- *Health risk assessment data (where applicable and consented)*
- Other information necessary for our functions and activities.

For **Employment Applications**, we may collect:

- Work history
- Skills
- Tax / *Superannuation / Banking* details
- *Employee health, medication (current) and vaccination records*
- References
- *Background check information (where permitted by law)*
- Other relevant information.

4.3 How We Collect Information

Where reasonable and practicable, we collect personal and health information directly from the individual through methods such as consent forms, chain of custody forms, or direct communication (in person, via telephone, *or secure digital platforms*). We may also collect information from third parties, such as authorised representatives or previous health professionals, with the individual's consent or as permitted by law. *We ensure third-party data collection complies with APPs and is transparent to the individual.*

4.4 Use and Disclosure of Information

We limit the disclosure of personal and health information and only disclose it for purposes such as:

- Management, funding, service monitoring, planning, evaluation, and complaint handling.
- Legislative and regulatory compliance.
- Quality assurance or clinical audit activities.
- Accreditation activities.
- Billing and debt recovery.
- Legal requirements (e.g., subpoenas or defence in legal proceedings).
- Activities directly related to providing health services where disclosure is reasonably expected.
- *Sharing de-identified data for research purposes, where permitted.*

For **transborder data flows**, disclosures may occur outside the individual's state, territory, or country, but only to organisations in jurisdictions with substantially similar privacy regimes *or where contractual safeguards ensure equivalent protection and are compliant with the requirements of the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APP).*

4.5 Storage and Security

Personal and health information is stored in paper and electronic forms. We take reasonable steps to protect this information, including:

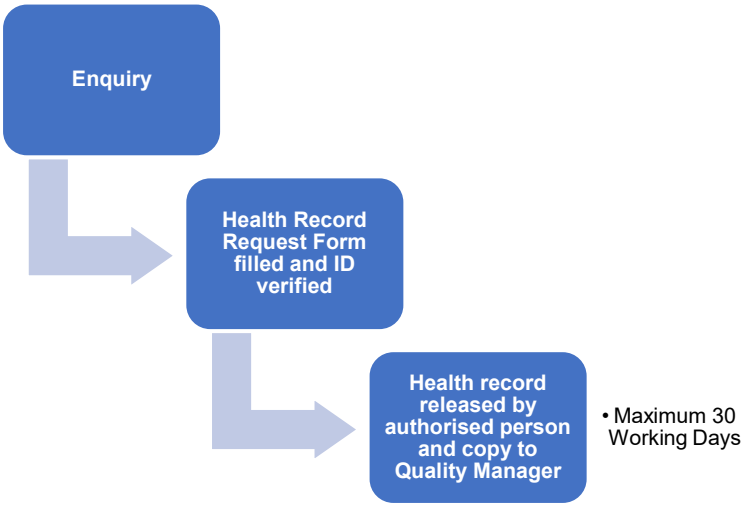
- Requiring staff to maintain confidentiality.
- Implementing document storage security measures.

- Enforcing security protocols for computer system access, *including encryption and multi-factor authentication where applicable.*
- Providing a discreet environment for confidential discussions.
- Verifying identity before granting access to personal or health information.
- Retaining information for the legally required period and disposing of it securely *in accordance with data destruction standards.*

4.6 Access to Personal Information

Individuals have the right to access their personal and health information under the Privacy Act 1988 (Cth), subject to exceptions (e.g., if access would threaten someone's life, health, or safety, impact another's privacy, or be unlawful). To request access, individuals can contact us at info@swhealth.com.au or visit our pre-employment medical centres. After identity verification, we will respond within *14 days, or 30 days for complex requests*. The process is as follows:

1. Submit a Health Record Request Form with verified identification.
2. An authorised person releases the health record, with a copy sent to the Quality Manager.
3. Access is provided within a maximum of 30 working days.



4.7 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 to queries, not for mailing lists or disclosure to third parties without consent (unless required by law).
- Providing aggregate, non-identifiable statistics about website usage to third parties.
- Not controlling the privacy practices of third-party websites linked from our site. Individuals are encouraged to review the privacy policies of those sites.

- *Implementing secure data transmission protocols (e.g., HTTPS) and regular security audits to protect online data.*

4.8 Complaints

Individuals who believe we have breached their privacy rights in any way or wish to discuss any issues about our privacy policy should contact the Quality Manager who will try to satisfy any questions and correct any errors on our part. If the Quality Manager is not able to satisfactorily answer an individual's concerns, the individual may contact the SW Health Head Office on 1300 795 227. The individual also has the right to make a complaint to the Privacy Commissioner on telephone number 1300 363 992 or in writing to:

Office of The Privacy Commissioner
GPO Box 5288, Sydney NSW 2001
or via fax, by sending it to +61 2 6123 5145.

https://www.oaic.gov.au/privacy/privacy-complaints/

---

5. Implementation and Responsibilities

5.1 Management Responsibilities

- Ensure compliance with the Australian Privacy Principles and state/territory privacy laws.
- Oversee the secure collection, storage, use, and disclosure of personal and health information.
- Provide training to employees on privacy obligations and confidentiality requirements.
- Address privacy complaints promptly and effectively.
- Maintain and update this policy as needed to reflect legal and operational changes *and emerging privacy standards*.

5.2 Employee Responsibilities

- Adhere to this policy and maintain the confidentiality of personal and health information.
- Collect, use, and disclose information only as permitted by this policy and applicable laws.
- Report any suspected privacy breaches to the Quality Manager immediately.
- Participate in privacy training and comply with security protocols for information handling.
- *Stay informed about updates to privacy policies and procedures.*

---

6. Forms

- GEN - FRM - 2150 - SWG – Health Record Request Form

---

7. Commitment Statement

SW Health is steadfast in its commitment to upholding the privacy rights of individuals while delivering high-quality services. By adhering to the Australian Privacy Principles and relevant state and territory laws, we ensure that personal and health information is handled with the utmost care, security, and transparency. *Our adoption of contemporary security measures and transparent processes reflects our dedication to maintaining trust in an increasingly digital world.* We encourage individuals to engage with us confidently, knowing their privacy is protected, and to reach out with any questions or concerns about our privacy practices.

Signed:

Matthew Holt
Managing Director
26 August 2025