Privacy Policy

CONTENTS

AUTHORISATION

Authorised by: Chief Executive Officer
Date Effective: 16 October 2025
Review/Consultation: Clinical Psychologist/General Manager – Healthcare & In-house Legal Counsel
Review Date: 16 October 2027

POLICY

Your Information and Your Privacy

This document explains how Harbison Health manages your personal information. We are committed to protecting your privacy in accordance with the *Australian Privacy Principles* under the *Privacy Act 1988* (Cth) and maintaining the confidentiality of your information as part of our professional and ethical obligations.

1. DEFINITIONS

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the information is true or false and regardless of whether the information is recorded in a material form or not.

Sensitive Information is a subset of personal information that includes health information about an individual, including information about their physical, mental or psychological health, disability, injury, genetic information, and information about health services provided to them.

Serious Harm includes physical, psychological, emotional, financial, or reputational harm that could have significant adverse effects on an individual's wellbeing or circumstances.

Privacy Officer means the designated person responsible for handling privacy matters and complaints for Harbison Health, being Ashley Stoyles.

2. WHAT INFORMATION WE COLLECT

We collect personal information necessary to provide you with quality health services. This includes:

Personal Details: Your name, address, date of birth, contact telephone numbers, Medicare number, emergency contact details, and payment information including details of any third-party payers such as insurance companies or employers.

Health Information: As part of providing health services, we collect and record health information relevant to your current situation and care. This includes information about your medical and mental health history, diagnoses, session notes, assessment results, treatment plans, medication information, reports from other health practitioners, and clinical observations. We may also collect information about your family medical history where relevant to your care.

Information from Others: We may collect personal information about you from referrers such as your GP, other health practitioners, employers, insurance companies, My Aged Care, government

agencies, or family members where you have consented or where it is reasonably expected as part of coordinated care.

3. HOW WE COLLECT YOUR INFORMATION

Your personal information is collected through various methods:

(a) Information you provide directly during appointments, assessments, and through forms, correspondence, emails, text messages, or telephone conversations with your clinician or our administration staff;

(b) Information received from other health practitioners through referrals, reports, correspondence, and as part of coordinated care arrangements;

(c) Information from third parties such as employers, insurance companies, or government agencies where you have provided consent or where collection is authorised by law; and

(d) In some circumstances, through video or audio recordings made as part of your treatment, which will only occur with your explicit consent.

If you believe any information we have recorded is incorrect, please discuss this with your clinician so we can investigate and make any necessary corrections.

4. PURPOSE OF COLLECTING AND USING YOUR INFORMATION

Your personal information is collected and used for the primary purpose of providing you with health services. This includes:

(a) Providing assessment, treatment, therapy, and other health interventions tailored to your needs and circumstances;

(b) Coordinating your care with other health professionals involved in your treatment, including your GP, specialists, or other allied health providers;

(c) Maintaining accurate clinical records that document your care and enable continuity of treatment over time;

(d) Preparing reports or assessments for other professionals, employers, insurance companies, or legal proceedings where you have provided consent;

(e) Complying with our legal and professional obligations, including mandatory reporting requirements, court orders, or statutory obligations under Australian law; and

(f) Quality improvement activities, clinical supervision, and professional development that enhance the services we provide, with information de-identified where possible.

5. CONSEQUENCES OF NOT PROVIDING INFORMATION

Health professionals are required to maintain clear and accurate records as part of their professional obligations and to ensure your safety and appropriate care. If you choose not to provide necessary personal information, we may not be able to:

(a) Provide you with appropriate health care services or fully meet your clinical needs;

(b) Coordinate your care effectively with other health professionals;

(c) Prepare reports or assessments requested by you or required by third parties; or

(d) Meet our legal obligations regarding your care and safety.

Please discuss any concerns about information collection with your treating clinician, who can explain why specific information is needed for your care.

6. CONFIDENTIALITY AND SHARING OF INFORMATION

Your personal information will remain confidential and will only be shared with your explicit consent, except in specific circumstances outlined below. When we seek your consent to share information, this includes:

(a) Sharing information with family members, carers, guardians, or other support people you have nominated;

(b) Communicating with other health professionals such as your GP, specialists, or other members of your care team;

(c) Providing written reports to employers, insurance companies, legal representatives, or other agencies where you have requested such reports; and

(d) Any other disclosure not specifically covered by the exceptions below.

Professional Supervision: Health professionals receive clinical supervision and consultation with colleagues as part of maintaining professional standards. When your information is shared in this context, all reasonable steps are taken to de-identify your information to protect your anonymity while enabling appropriate professional oversight.

7. EXCEPTIONS TO CONFIDENTIALITY

There are limited circumstances where we may share your information without obtaining your consent:

(a) **Legal Requirements:** When required by law, court order, subpoena, or other legal process, or where disclosure is authorised under Australian legislation;

(b) **Mandatory Reporting:** When we are legally required to make mandatory reports, including child protection concerns, elder abuse, or other statutory reporting obligations;

(c) **Serious Harm Prevention:** When we reasonably believe that disclosure is necessary to prevent or lessen a serious or imminent threat to your life, health, or safety, or to the life, health, or safety of another person or the public;

(d) **Law Enforcement:** When disclosure is reasonably necessary for law enforcement activities or where we reasonably believe unlawful activity has been, is being, or may be engaged in; and

(e) **Professional Oversight:** When required for professional registration, complaints processes, or investigation of professional conduct matters.

8. DATA SECURITY AND STORAGE

We take comprehensive measures to protect your personal information from misuse, loss, unauthorised access, modification, or disclosure. Our security framework includes:

(a) **Access Controls:** All electronic systems require individual user authentication with secure passwords, and two-factor authentication is implemented for access to sensitive information systems;

(b) **Data Classification:** Information is classified according to sensitivity levels, with health information requiring additional authorisation to access and being stored separately from general personal information;

(c) **Encryption:** Personal information is encrypted both during transmission and when stored electronically to prevent unauthorised access;

(d) **Physical Security:** Paper-based records are stored in locked, secure areas with controlled access, and workstations are secured when not in use;

(e) **Regular Audits:** We regularly review and audit our security measures, access logs, and authorised users to ensure systems remain secure and access is appropriate;

(f) **Backup and Recovery:** Secure backup systems ensure information can be recovered in the event of system failure while maintaining security protections; and

(g) **Secure Disposal:** Electronic and paper records are securely destroyed when no longer required, in accordance with professional record-keeping requirements and legal obligations.

9. OVERSEAS DISCLOSURE OF INFORMATION

All personal data collected by our organisation is securely stored in Australia. We utilise reputable cloud storage providers to ensure the secure storage and backup of this data.

We will only send your personal information to recipients outside Australia in the following circumstances:

(a) With your express written consent for the specific overseas disclosure; or

(b) For secure data storage and backup purposes using reputable cloud storage providers that maintain security standards equivalent to Australian requirements and are bound by contractual obligations to protect your information in accordance with the *Australian Privacy Principles*.

Before any overseas disclosure, we take reasonable steps to ensure the recipient complies with privacy protections substantially similar to those required under Australian privacy law.

10. ANONYMITY AND PSEUDONYMS

Where it is lawful and practicable, we will provide you with the option of not identifying yourself or using a pseudonym when accessing our services. However, in most cases, we need to collect and use your real name and identifying information to:

(a) Provide appropriate clinical care and maintain accurate health records;

(b) Coordinate your care with other health professionals;

(c) Meet our professional and legal obligations; and

(d) Process Medicare claims or insurance payments where applicable.

11. USE OF GOVERNMENT IDENTIFIERS

We collect and use government-issued identifiers such as Medicare numbers only when necessary for the provision of health services, processing payments, or meeting our legal obligations. We do not use government identifiers for our own internal identification systems unless specifically required or authorised by law.

12. ACCESSING AND CORRECTING YOUR INFORMATION

You have the right to request access to the personal information we hold about you and to request corrections if you believe the information is inaccurate, incomplete, outdated, irrelevant, or misleading.

Access Requests: To access your information, you may discuss this directly with your clinician or make a written request to our Privacy Officer. We will respond to written requests within 30 days and may arrange an appointment with your clinician to discuss the information if necessary for clarification.

Corrections: If you believe information we hold about you is incorrect, please inform your clinician or our administration staff. We will investigate your concerns and take reasonable steps to correct the information where we are satisfied it is inaccurate, out of date, or incomplete.

Refusal of Access or Correction: We may refuse access to your information or decline to make corrections in limited circumstances, including where:

(a) Providing access would pose a serious threat to the life, health, or safety of any person, or to public health or safety;

(b) Access would have an unreasonable impact on the privacy of other individuals;

(c) The request is frivolous, vexatious, or unreasonable;

(d) The information relates to legal proceedings between us and access would not be available through normal legal discovery processes;

(e) Access is prohibited under Australian law or court order; or

(f) Where providing access would reveal information provided in confidence or prejudice law enforcement activities.

Where we refuse access or correction, we will provide you with written reasons and information about how to make a complaint about our decision.

13. RETENTION AND DESTRUCTION OF INFORMATION

We retain your personal information only for as long as necessary to provide you with ongoing health services and to meet our professional and legal obligations. Clinical records are retained for a minimum period as required by professional standards and legal requirements, typically seven years for adults and until age 25 for individuals who were minors when treated.

When information is no longer required, it is securely destroyed through approved methods that ensure the information cannot be recovered or reconstructed.

14. DATA BREACH RESPONSE

In the event of unauthorised access, disclosure, or loss of your personal information that is likely to result in serious harm, we will:

(a) **Immediate Response:** Contain the breach and conduct a preliminary assessment to determine the scope and cause of the incident;

(b) **Risk Assessment:** Evaluate whether the breach is likely to result in serious harm to affected individuals, considering factors such as the sensitivity of the information, the nature of affected individuals, the identity of persons who may have gained access, and whether safeguards such as encryption were in place;

(c) **Investigation:** Conduct a thorough investigation within 30 days to determine the full extent of the breach and appropriate response measures;

(d) **Remediation:** Take immediate action to prevent further unauthorised access and implement remedial measures to reduce the risk of harm;

(e) **Notification to Regulator:** If the breach is likely to result in serious harm (an "eligible data breach"), notify the Office of the Australian Information Commissioner as soon as practicable, including details of the breach, affected information, and remedial action taken;

(f) **Individual Notification:** Notify affected individuals directly of eligible data breaches as soon as practicable, providing information about the breach, potential consequences, and recommended steps they can take to protect themselves;

(g) **Record Keeping:** Maintain comprehensive records of the incident, investigation findings, remedial actions, and notifications made; and

(h) **Prevention:** Review and strengthen our security measures and procedures to prevent similar incidents occurring in future.

15. WORKFORCE OBLIGATIONS

All members of our workforce, including employees, contractors, and volunteers, are required to:

(a) Complete privacy and confidentiality training as part of their orientation and ongoing professional development;

(b) Sign confidentiality agreements that bind them to protect the privacy and confidentiality of all personal information they may encounter;

(c) Follow our privacy policies and procedures in all their professional activities;

(d) Report any suspected privacy breaches or security incidents immediately to their supervisor or the Privacy Officer; and

(e) Only access personal information that is necessary for their role and responsibilities.

16. COMPLAINTS AND PRIVACY OFFICER

If you have concerns about how we have handled your personal information, we encourage you to raise these with us directly so we can address your concerns promptly.

Privacy Officer Contact Details:

Name: Ashley Stoyles
Phone: 02 4868 6208
Email: privacy@harbisoncare.org.au

Internal Complaints Process:

(a) You may make a complaint directly to your clinician, our administration staff, or our Privacy Officer;

(b) All complaints will be acknowledged within 48 hours of receipt;

(c) We will investigate your complaint and provide you with a written response within 28 days, or notify you if additional time is required with reasons for the delay;

(d) Our response will include our findings, any action we will take to address your concerns, and information about external complaint options if you are not satisfied with our response; and

(e) We will implement any necessary changes to prevent similar issues occurring in future.

External Complaints:

If you are not satisfied with our response to your privacy complaint, you may lodge a complaint with the Office of the Australian Information Commissioner (**OAIC**):

Phone: 1300 363 992
Website: www.oaic.gov.au
Online complaint form: https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us
Post: Office of the Australian Information Commissioner, GPO Box 5218, Sydney NSW 2001

17. UPDATES TO THIS POLICY

This privacy policy may be updated from time to time to reflect changes in our practices, legal requirements, or to improve clarity. We will notify clients of significant changes and make the current version available on our website and at our premises.

18. FURTHER INFORMATION

If you would like more information about privacy laws and your rights, you can obtain additional resources from:

(a) The Office of the Australian Information Commissioner at www.oaic.gov.au;

(b) Our Privacy Officer, who can provide information about how this policy applies to your specific circumstances; or

(c) Your treating clinician, who can explain how privacy protections relate to your clinical care.

This policy was last updated on 16/10/2025 and will be reviewed regularly to ensure it remains current and comprehensive.

Contact Information:

Harbison Health
PO Box 349, Bowral 2576
Phone: 02 4868 6486

Harbison Privacy Officer

Ashley Stoyles - 02 4868 6208