Harbison Consumer Privacy Policy

Harbison ACN 001 507 624 (**we, us, our**) is committed to protecting the privacy of individuals. As an approved aged care provider in New South Wales, we recognise the importance of handling personal information with the utmost care, particularly for our residents, their families, and other stakeholders. This Privacy Policy sets out how we collect, use, disclose, store, and protect personal information in accordance with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

This Policy applies to all personal information we handle, including through our website, interactions at our facilities, and service provision. It is designed to be transparent and accessible, ensuring residents and their families understand how their privacy is safeguarded. We regularly review this Policy to reflect changes in law and practice.

1. Your Consent

By using our website or engaging with our services, you consent to us collecting, using, and disclosing your personal information in accordance with this Policy. Consent is obtained where required, and we will always seek consent for sensitive information unless an exception applies (e.g., where it is impracticable or unreasonable, such as in emergencies or for legal obligations under the *Aged Care Act 2024* (Cth)).

We do not collect personal information without consent unless authorised by law, such as for health service provision. You may withdraw consent at any time by contacting our Privacy Officer.

2. Personal Information Collected by Us

Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and recorded in material form. This includes sensitive information (e.g., health details, racial or ethnic origin).

As an approved aged care provider, we collect personal information necessary for delivering residential care, including health services. We do not collect more than is reasonably necessary for our functions.

Categories of Personal Information

For Residents and Prospective Residents:

- Identification:
  - Name, date of birth, address, contact details, Medicare number, and emergency contacts (including Person Responsible).
- Health and Medical Information:
  - Medical history, vaccination status (e.g., influenza, COVID-19), allergies, medications, pathology results, care plans, assessments, and genetic information where relevant to care.
- Financial and Administrative:
  - Billing details, funding sources (e.g., AN-ACC, NDIS plans), and entitlement information.

- Social and Cultural:
    - Religious beliefs, cultural background, family details for personalised care. We obtain explicit consent unless impracticable.
- Care and Services:
    - Details on daily living needs, mobility, cognitive status, and preferences to support dignity of choice.

For Family Members, Visitors, and Other Stakeholders:

- Contact details and relationship to resident.
- Feedback or complaints submitted via forms or surveys.
- Website interactions:
    - IP address, browser type, pages visited, and referral sources (anonymised where possible).

For Workforce (Employees, Contractors, Volunteers):

- Employment details:
    - Name, address, tax file number, superannuation, qualifications, and references.
- Health and Safety:
    - Vaccination records, fitness for work assessments (limited to role requirements under *Work Health and Safety Act 2011* (Cth)).
- Training and Compliance:
    - NDIS Worker Screening Check or National Police Certificate results.

We collect this information directly from you (e.g., admission forms, website submissions) or indirectly (e.g., from medical professionals with consent). Unsolicited information is destroyed or de-identified if not needed.

3. Disclosure of Personal Information

We disclose personal information only as necessary for providing aged care services. Disclosures are limited to what is reasonably expected and authorised by law. We do not sell or rent personal information.

Permitted Disclosures

For Care and Treatment:

- To healthcare professionals (e.g., GPs, specialists, hospitals) involved in your care, with consent or where necessary for health services (e.g., sharing care plans).
- To allied health providers or pharmacies for medication management.
- To funding bodies (e.g., Services Australia, NDIS Commission) for subsidy claims.

For Quality and Safety:

- To the Aged Care Quality and Safety Commission (**ACQSC**) for reporting incidents under the Serious Incident Response Scheme (**SIRS**), including neglect or abuse.
- Anonymised data for audits or quality improvement.

For Legal and Regulatory Compliance:

- To regulators (e.g., NSW Health, ACQSC, NDIS Quality and Safeguards Commission) or law enforcement if required by law.
- To insurers for claims processing.
- In emergencies, to protect life or health, e.g., disclosing to paramedics without consent if the resident lacks capacity.

Website and Digital Disclosures:

- Aggregated, de-identified data to analytics providers (e.g., Google Analytics) for site improvement (see below).
- No sharing with unrelated third parties without consent.

We do not disclose sensitive information unless consented to or permitted (e.g., for public health). All disclosures are documented.

4. Protecting Your Personal Information

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. We prioritise security in a vulnerable environment.

Security Measures

- Physical Security:
  - Paper records are stored in locked cabinets; facilities access is controlled via keycards and CCTV (see Surveillance section).
- Electronic Security:
  - Data is encrypted (e.g., health records); access is role-based with multi-factor authentication. All health data is stored in My Health Records.
- Transmission:
  - Information shared electronically (e.g., with GPs) uses secure portals (e.g., My Health Record) or encrypted email.
- Retention:
  - We retain information only as long as needed for care (up to 7 years post-discharge under health records laws) or legal requirements (e.g., 15 years for certain financial records). Records are securely destroyed or de-identified thereafter.
- Breach Response:
  - If a data breach occurs, we follow the Notifiable Data Breaches scheme (Privacy Act). We assess harm risk and notify affected individuals and the OAIC if serious harm is likely (e.g., identity theft risk). Notifications include breach details and protective steps (e.g., monitoring credit reports).

We conduct regular audits and staff training to ensure compliance. In case of a breach, contact our Privacy Officer immediately.

Surveillance

We use CCTV in common areas of our facilities for security purposes. CCTV footage is not audio-recorded, and we do not use listening devices. Signs are displayed in visible locations to inform individuals of CCTV presence. Footage is accessed only by authorised personnel

for legitimate purposes (e.g., incident investigation) and is stored securely for a limited period before deletion. We do not use surveillance to monitor private conversations or activities. Access to footage is logged, and we adhere to privacy laws regarding data handling. If you have concerns about surveillance, please contact our Privacy Officer.

Nobi Smart Lights

Devices have been installed in selected areas in our organisation. These devices are activated only after consultation and informed consent. In the event of a fall, data is securely stored for 14 days to support incident management, after which it is automatically deleted from the device.

5. Cookies

Cookies are small data files stored on your device's browser to enhance website functionality. We use them to:

- Analyse site usage (e.g., Google Analytics cookies track pages visited, time spent, and referral sources for aggregated insights).
- Remember preferences (e.g., language settings).
- Enable essential functions (e.g., form submissions).

We do not use cookies to collect sensitive information without consent. You can manage cookies via browser settings (e.g., disable third-party cookies in Chrome or Safari). Disabling may affect site features.

We comply with APPs for transparency and do not share cookie data with third parties except as outlined (e.g., anonymised analytics with Google under data processing agreements).

6. Web Beacons

We do not currently use web beacons on our website. If implemented, they would track non-personal data (e.g., email opens) for service improvement, with opt-out options provided.

7. Overseas Disclosure

As an NSW-based provider, most processing occurs in Australia. However, some IT support or analytics may involve overseas recipients (e.g., Microsoft servers in the USA). As reasonably practical, we ensure these recipients are bound by similar privacy laws (e.g., via contractual clauses compliant with OAIC guidelines) and take reasonable steps to protect data (e.g., encryption). No health data is stored overseas without explicit consent or legal necessity.

If disclosure is required (e.g., international referrals), we notify you and obtain consent where practicable.

8. Third Parties

We may share personal information with third parties only for permitted purposes, such as:

- Service providers (e.g., laundry, maintenance contractors) under strict confidentiality agreements.
- Aged care assessors or allied health via secure portals.
- Auditors or insurers for compliance/funding.

We do not share your personal information with unrelated parties without consent.

9. Accessing and Managing Your Personal Information

You have the right to access your personal information held by us. Requests can be made in writing to our Privacy Officer privacy@harbison.com.au. We will respond within a reasonable period, providing access unless an exception applies (e.g., health/safety risks).

To request access:

- Submit a form (available via Privacy Officer);
- Provide identification to verify your request; and
- Specify the information sought and preferred format (e.g., digital copy).

We may charge reasonable fees for access (e.g., photocopying), but not for the request itself. If denied, we explain reasons and appeal options (e.g., to the Administrative Review Tribunal).

For correction, contact us if information is inaccurate/out-of-date. We will correct within 30 days or explain refusal. Updates are notified to recipients where practicable.

10. Complaints

We value your feedback and handle complaints seriously. If you believe we have breached the Privacy Act or this Policy:

Internal Complaints:

- Contact our Privacy Officer, in writing via privacy@harbison.com.au or by phone (details below). We aim to resolve within 30 days.
- For aged care-specific issues (e.g., care privacy), use our internal grievance process under the Aged Care Quality Standards.

External Complaints:

- Escalate to the OAIC (www.oaic.gov.au, 1300 363 992) for Privacy Act matters.
- For aged care complaints (e.g., privacy in care), contact the Aged Care Quality and Safety Commission (www.agedcarequality.gov.au, 1800 951 822).
- If under NDIS, contact the NDIS Commission (www.ndiscommission.gov.au, 1800 035 544).

We cooperate fully with investigations and do not charge for complaints.

11. Variations

We may review and update this Policy to reflect legal changes or operational needs. The current version is available on our website (www.harbison.com.au/privacy) and at

reception. We will notify you of material changes via website notice or direct communication where practicable.

12. Further Information

For more details or to exercise your rights, contact:

Privacy Officer
Phone: 02 4868 6208
Email: privacy@harbison.com.au
Address: 2 Charlotte Street, Burradoo NSW 2576

Refer to OAIC resources (www.oaic.gov.au/privacy) or the Aged Care Quality and Safety Commission (www.agedcarequality.gov.au) for general privacy guidance.

Harbison reserves the right to vary this Policy without notice, but we commit to transparency.