

Privacy and Confidentiality Policy Template

Purpose:

To ensure that all personal, health, and sensitive information about residents, staff, and stakeholders is managed securely, lawfully, and confidentially in accordance with the Aged Care Quality Standards, the Privacy Act 1988 (Cth), and other regulatory requirements.

Scope:

Applies to all employees, contractors, volunteers, and healthcare professionals who collect, access, use, or disclose personal or sensitive information within the organisation.

Policy Statement:

The organisation is committed to:

- Protecting the privacy, confidentiality, and dignity of all individuals.
- Managing personal information transparently and securely.
- Complying with the Australian Privacy Principles (APPs) and Aged Care Quality Standards.
- Ensuring residents are informed and provide consent regarding information collection, use, and disclosure.
- Responding promptly to privacy breaches or complaints.

Legislative Context:

- Privacy Act 1988 (Cth)
- Aged Care Act 1997 (Cth)
- Aged Care Quality Standards (Standard 1 – The Person; Standard 2 – The Organisation)
- Quality of Care Principles 2014
- Freedom of Information Act 1982 (Cth)
- Data Breach Notification obligations under the Notifiable Data Breaches Scheme

Definitions:

- **Personal Information:** Information about an identified individual, including health, contact, and personal data.
- **Confidentiality:** The safeguarding of information from unauthorised disclosure.
- **Sensitive Information:** Includes health, racial or ethnic origin, religious, sexual orientation, or biometric data.
- **Breach:** Unauthorised access, disclosure, or loss of personal information.

Key Principles:

1. Information is collected only when necessary for care or operational purposes.
2. Informed consent is obtained for the collection and disclosure of personal data.
3. Residents can access or request correction of their data at any time.
4. Staff are responsible for maintaining confidentiality and following secure data handling practices.
5. Data is stored, transmitted, and disposed of securely.
6. Any privacy breaches are reported and addressed promptly with corrective action.

Responsibilities:

- **Approved Provider / Board:** Ensure compliance with privacy laws and accountability for organisational data protection.
- **Quality & Compliance Manager:** Oversee privacy systems, breach management, and staff training.
- **Facility Manager:** Implement privacy procedures and ensure documentation security.
- **All Staff:** Maintain confidentiality and follow the privacy and record management guidelines.
- **IT / Data Management Personnel:** Ensure digital records and systems have adequate security controls.

Procedures:

1. Collect personal information directly from the resident or representative unless impractical.
2. Obtain written or verbal consent before disclosure to third parties.
3. Store physical records in locked cabinets and restrict digital access to authorised users only.
4. Ensure electronic records have password protection and encryption where applicable.
5. Dispose of obsolete records by shredding or secure deletion.
6. Report privacy breaches immediately to the Quality & Compliance Manager for investigation.
7. Respond to information access requests within a reasonable timeframe (typically 30 days).

Privacy Breach Response:

- Contain the breach and assess potential harm.
- Notify affected individuals where required.
- Report notifiable breaches to the Office of the Australian Information Commissioner (OAIC).
- Review and strengthen systems to prevent recurrence.

Monitoring and Review:

- Annual review of privacy compliance and data protection processes.
- Regular audits of record-keeping and digital security systems.
- Staff training on privacy awareness conducted annually or as required.

Associated Policies:

- Information Management Policy
- Data Security and ICT Policy
- Feedback and Complaints Management Policy
- Risk Management Policy
- Incident Management and Reporting Policy

Evidence and Records:

- Consent forms and resident information records
- Access and correction logs
- Privacy breach reports
- Privacy training attendance records
- Secure disposal certificates

Policy Control:

Version	Effective Date	Review Date	Policy Owner	Approved By	Status
1.0	20 January 2026	20 January 2027	Quality & Compliance Manager	Approved Provider Board	Draft

Compliance Summary:

Entity Type	Entity Name	Completion Rate	Status
Policy	Privacy and Confidentiality Policy	100%	FULLY COMPLIANT (100%)