

Privacy and Confidentiality Policy

PURPOSE

Physio Inq Pty Ltd TA Pinq Care is committed to protecting the privacy, confidentiality and dignity of all individuals receiving aged care and support service.

This policy ensures that all personal, health and organisational information is handled lawfully, ethically, and respectfully – supporting the delivery of safe, high-quality, and person-centred care in line:

- The Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)
- The Aged Care Act 2024 and Aged Care Quality and Safety Commission Act 2018
- The Strengthened Aged Care Quality Standards (2025).

This policy supports compliance with:

- Standard 1 (The Individual)
- Standard 2 (The Organisation)
- Standard 8 (Governance).

SCOPE

This policy applies to:

- All Pinq Care employees and associated providers.
- All personal and sensitive information collected from participants, families, employees, and business partners.
- All operational, clinical, financial, and governance records in both electronic and hard-copy form.

KEY DEFINITIONS

- **Personal Information:** Information or an opinion about an identifiable individual, whether true or not, and whether recorded in a material form or not.
- **Sensitive Information:** A subset of personal information that includes details about a person's health, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, or criminal record.
- **Health Information:** Details about an individual's health status, disabilities, or health services provided.
- **Confidential Information:** Non-public information obtained through employment or service delivery, including business, financial, or participant information.

- **Notifiable Data Breach (NDB):** A data breach likely to result in serious harm that must be reported to affected individual and the Office of the Australian Information Commissioner (OAIC).

POLICY STATEMENT

Pinq Care values the trust placed in us to handle personal information responsibly and respectfully. We will:

- Collect, use, store, and disclose personal information only for legitimate purposes including care delivery, employment, or compliance.
- Obtain informed consent before collecting, using, or disclosing information, except where disclosure is required by law.
- Protect information through secure systems (e.g. AlayaCare, Microsoft 365, SharePoint, Teams) with encryption, authentication and role based access controls.
- Ensure information is accurate, current and complete, and accessible to the individual upon request.
- Manage privacy and confidentiality breaches in line with Notifiable Data Breaches Scheme (Privacy Act 1988), including notification to affected participants and the Office of the Australian Information Commissioner (OAIC) where required.
- Ensure access to personal information is restricted to authorised personnel, monitored, and reviewed regularly.
- Record suspected or confirmed breaches in the Incident Register to ensure oversight and governance.
- Provide training and awareness to staff on privacy obligations and confidentiality principles.
- Require associated providers to comply with Pinq Care's privacy and confidentiality standards.

INFORMATION COLLECTION AND USE

Information is collected directly from the individual or their authorised representative, and with consent, from health professionals, service providers or government agencies.

Information collected may include:

- Personal identifiers (e.g. name, contact details, date of birth)
- Health, medical and care information
- Financial details necessary for billing, subsidies or payroll.
- Employment and credentialing information for staff.

Information is used only for:

- Delivering aged care and support services

- Employment and HR administration
- Meeting funding, billing and compliance obligations.
- Quality assurance, audits and internal reporting.
- Meeting legal or safeguarding obligations

INFORMATION STORAGE AND SECURITY

- Information is stored within Australian-based cloud systems (e.g. Microsoft Azure, Microsoft 365, and AlayaCare) protected by encryption, access controls, and multifactor authentication.
- Access is limited to authorised personnel and monitored by the IT team.
- Hard-copy documents are stored in locked facilities and securely destroyed when obsolete, in accordance with the Records Management Policy.
- System backups, disaster recovery, and audit logs are maintained to protect data integrity and prevent unauthorised disclosure.

RETENTION AND DISPOSAL

Records are retained for the period required by legislation and contractual requirements and securely destroyed or de-identified once retention period ends.

SOCIAL MEDIA AND MARKETING

Pinq Care may use de-identified testimonials, photos, or videos for education or promotional purposes only with written consent from the participant or their authorised representative.

Consent can be withdrawn at any time by contacting Pinq Care, after which materials will be removed promptly.

BREACH MANAGEMENT AND REPORTING

All suspected or confirmed privacy breaches must be reported immediately to the Executive General Manager.

The Executive General Manager, with support from IT and Quality, will:

1. Conduct an initial assessment to determine if the breach is notifiable.
2. Notify affected individuals and, if required, the Office of the Australian Information Commissioner and Aged Care Quality and Safety Commission where required.
3. Record the breach in the Incident Register and track corrective actions in the Pinq Improvement Register.
4. Implement system and procedural improvements to prevent recurrence.

RIGHTS AND COMPLAINTS

Participants and employees have the right to:

- Access personal information held about them.
- Request correction of inaccurate or outdated information.
- Make a complaint about the handling of personal or confidential information.

Requests and complaints can be directed to Pinq Care:

Email: feedback@pinqcare.com.au

Postal: [5/20 Cliff St, Milsons Point NSW, 2061 Australia](#).

If you are not satisfied with the outcome, you may contact:

- Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au
- Aged Care Quality and Safety Commission: www.agedcarequality.gov.au

GOVERNANCE AND OVERSIGHT

Governing Body: Holds ultimate accountability for privacy, confidentiality and information security compliance.

Executive General Manager: Ensures ongoing compliance and review of this policy and ensure breaches are investigated and reported in line with incident management requirements.

Information Technology (IT) Manager / IT Team: Maintains secure systems, monitors access, manages cybersecurity controls and incident response.

Care Partner: Obtains participant consent, ensure secure data handling and reports breaches.

People and Culture Manager: Manages secure storage of employee records and compliance documentation.

Employees: Maintain confidentiality and protect personal and health information accessed during daily practice, use consent forms correctly and immediately report suspected or confirmed breaches.

Associated Providers: Must comply with Pinq Care's privacy and confidentiality obligations.

LEGISLATION AND STANDARDS

Privacy Act 1988 (including the Australian Privacy Principles)

Aged Care Act 2024

My Health Records Act 2012

Aged Care Quality and Safety Commission Act 2018

Strengthened Aged Care Quality Standards (2025)

RELATED DOCUMENTS

Information Management Policy
Records Management Policy
Incident Management Policy
Risk Management Policy
Continuous Improvement Policy

REVIEW

This policy will be reviewed annually or sooner if required by changes in legislation, regulation or organisational structure. Outcomes of incidents, complaints, and audits will inform future updates to promote continuous improvement.

Document Name	Privacy and Confidentiality Policy
Document Number	PINQC-P-001
Version	1.0
Approved by	Executive General Manager – Aged Care
Approval Date	29/10/2025
Review Date	29/10/2026