WebCAS Privacy Management Plan

System: WebCAS
Version: 2.15
Document Owner: OCI
Effective Date: 15/01/2026
Review Date: Annually

---

1. Purpose

This Privacy Management Plan describes how WebCAS manages personal and health information throughout its lifecycle.

The system supports the registration, enrolment, administration and ongoing management of participants attending health-related exercise programs. The system does not store any banking details. The organisation is committed to protecting participant privacy and ensuring compliance with applicable privacy legislation, including the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

---

2. Scope

This plan applies to:

- all users of the system
- administrative staff
- instructors
- clinical staff (where applicable)
- contractors
- software developers
- system administrators
- third-party service providers.

The plan covers all information collected, stored, processed and disclosed through the enrolment system.

---

3. Privacy Objectives

The objectives of this plan are to:

- protect participant privacy
- safeguard health information
- ensure lawful collection and use of information
- minimise privacy risks
- support secure delivery of health exercise services
- comply with relevant legislation and contractual obligations.

4. Information Collected

The system may collect the following information.

Participant Identification

- Full name
- Date of birth
- Gender
- Residential address
- Postal address
- Email address
- Telephone number
- Emergency contact details

Health Information

Where required to safely deliver exercise programs:

- Medical conditions
- Exercise limitations
- Injury history
- Mobility information
- Falls risk
- Relevant diagnoses
- GP or referrer details
- Allied health provider details
- Medical clearances
- Exercise restrictions
- Disability information
- NDIS participant details (where applicable)

Only information necessary for safe participation is collected.

Administrative Information

- Enrolment records
- Attendance records
- Program history
- Waiting list status
- Payment status (if applicable)
- Consent records
- Communication preferences

Technical Information

- Login history
- User account details
- IP addresses

- Device information
- Audit logs
- System activity logs

---

5. Purpose of Collection

Information is collected to:

- assess participant eligibility
- manage class enrolments
- allocate participants to suitable exercise programs
- ensure participant safety
- communicate with participants
- manage attendance
- contact emergency contacts where necessary
- provide reports to authorised health providers where consent has been provided
- meet legal and funding obligations
- improve service delivery.

Health information is collected only where reasonably necessary for providing safe exercise services.

---

6. Collection Principles

Information is collected:

- directly from participants wherever possible
- from authorised representatives where appropriate
- from referring health professionals with consent
- only where necessary
- using clear privacy notices.

Participants are informed:

- what information is collected
- why it is collected
- how it will be used
- who it may be shared with
- how to access or correct their information.

---

7. Consent

Participants provide consent before:

- collection of health information
- sharing information with health professionals

- receiving marketing communications
- participation in exercise programs where health information is required.

Consent records are stored within the system.

Participants may withdraw consent where permitted by law.

---

8. Access Control

Access is restricted according to user roles.

Examples include:

Role	Typical Access
Reception Staff	Participant registration and contact information
Exercise Instructor	Class lists and relevant health information required for safe exercise supervision
Clinical Staff	Full participant records where clinically required
System Administrator	Technical administration only
Management	Reporting and operational information

Access follows the principle of least privilege.

---

9. Information Security

Security controls include:

Authentication

- unique user accounts
- strong password requirements
- automatic account lockout

Data Protection

- encryption in transit
- encryption at rest
- secure backups
- secure cloud storage

Monitoring

- audit logging
- login monitoring
- failed login alerts
- privileged access monitoring

Software Security

- secure software development
- regular patching
- vulnerability management
- penetration testing
- malware protection

---

10. Disclosure of Information

Participant information is disclosed only where authorised.

Examples include:

- treating health professionals
- referring clinicians
- emergency services
- government funding bodies where required
- authorised contractors supporting the system.

Information is never sold or disclosed for unrelated commercial purposes.

---

11. Data Retention

Records are retained in accordance with:

- applicable legislation
- funding requirements
- health record retention obligations
- organisational record management policies.

At the end of the retention period, information is securely destroyed or permanently de-identified.

---

12. Participant Rights

Participants may request:

- access to their information
- correction of inaccurate records
- updates to contact information
- withdrawal of consent where applicable
- information about how their information is used
- copies of privacy notices.

Requests are handled within legislative timeframes.

13. Privacy by Design

Privacy is incorporated into system development by:

- collecting only necessary information
- limiting mandatory fields
- implementing role-based access
- encrypting sensitive information
- maintaining comprehensive audit logs
- regularly reviewing data collection practices
- conducting Privacy Impact Assessments before major changes.

---

14. Privacy Incidents

Examples include:

- unauthorised access
- accidental disclosure
- loss of participant information
- ransomware attacks
- compromised user accounts
- incorrect disclosure of health information.

All incidents are:

1. identified
2. contained
3. investigated
4. risk assessed
5. reported where required
6. documented
7. reviewed for improvement.

Eligible data breaches are managed in accordance with the Notifiable Data Breaches scheme.

---

15. Third-Party Providers

Where cloud hosting or third-party services are used, providers must:

- maintain appropriate security controls
- protect participant information
- comply with contractual privacy obligations
- notify the organisation of security incidents
- permit security reviews where appropriate.

16. Staff Responsibilities

All authorised users must:

- protect participant confidentiality
- use information only for authorised purposes
- report suspected privacy breaches
- maintain secure passwords
- log out of unattended devices.

---

17. Governance

The Privacy Officer is responsible for:

- monitoring privacy compliance
- responding to participant enquiries
- managing complaints
- overseeing privacy incidents
- maintaining this Privacy Management Plan
- coordinating Privacy Impact Assessments.

---

18. Review

This plan will be reviewed:

- annually
- following major software upgrades
- following legislative changes
- following a privacy incident
- after significant changes to data collection practices.
