Altura Health Data Storage & Security Policy

This policy explains, at a high level, how Altura Health safeguards information to prevent loss, unauthorised access, or misuse. It also outlines our approach to backups and restoration.

Data Storage and Residency

- Customer data is hosted in Australia using AWS.
- Data is encrypted in transit and at rest using industry-standard encryption.
- Access to systems and customer data is controlled using least privilege principles and role-based access.

Data Governance and Handling

- Data access is restricted to authorised personnel and governed by documented processes.
- Logging and auditability controls support traceability and accountability.
- Data retention and deletion are managed in line with contractual and regulatory obligations.

Backups and Restoration

- Backups are performed regularly using cloud-native services.
- Backups frequency and retention vary depending on the product, environment, and data type (e.g. databases vs documents).
- Backup storage is protected using access controls and safeguards to reduce the risk of unauthorised access, deletion or modification.
- Restoration procedures are documented and maintained. Recovery time depends on the nature of the incident and the impacted component.

Monitoring and Assurance

- Operational monitoring is used to support backup integrity and availability.
- Periodic backup checks and restore testing are performed to validate recoverability.

Security Assurance

- Altura Health undertakes regular independent security testing (e.g. penetration testing and security assessments) with third-party specialists.
- A summary of recent security assessment results may be provided on request, subject to

appropriate confidentiality arrangements.

Account Access

- Altura Health Supports Single Sign-On (SSO) where configured and enforces Multi-Factor Authentication (MFA) for account access.
- Altura Health supports RBAC, and each facility decides the role structure and is responsible for assigning and maintaining user access for their team.
- Authentication and access controls may vary depending on customer configuration and agreed requirements.