Security & Compliance Policy

Document Name	Security & Compliance Policy
Version	1.0
Effective Date	September 2025
Applies To	All MediMap Customers in AU and NZ
Prepared By	MediMap Support
Approved By	Head of Product & Delivery

Introduction

MediMap provides SaaS-based digital medication management services for healthcare organisations in New Zealand and Australia. We understand our role in protecting sensitive health information and maintaining the trust of providers, prescribers, and residents. This statement outlines how MediMap safeguards data security and complies with AU and NZ health data requirements.

1. Compliance Commitments

MediMap complies with:

- NZ Privacy Act 2020 & Health Information Privacy Code 2020
- AU Privacy Act 1988 (Cth) & Australian Privacy Principles (APPs)
- My Health Records Act 2012
- State/Territory health privacy legislation where applicable
- We also align our controls with ISO/IEC 27001 and the Australian Cyber Security Centre's Essential Eight.

2. Data Sovereignty & Hosting

- NZ customers: Data is hosted exclusively within New Zealand data centers.
- AU customers: Data is hosted exclusively within Australian data centers.
- No offshore transfers of identifiable health data occur without explicit customer consent.
- Daily encrypted backups are stored in multiple domestic data centers for resilience.

3. Backup & Disaster Recovery

MediMap Data Backup & Security:

- Daily full backups of all critical data.
- Incremental backups every 15 minutes to minimise data loss.
- 90-day rolling retention of backups.
- Backups are encrypted with AES-256 and transmitted via TLS 1.2+.
- Disaster recovery testing is conducted regularly to validate recovery time (RTO) and recovery point objectives (RPO).

4. Security Controls

- Access Management: Role-based access control (RBAC) with multi-factor authentication for all privileged users.
- Audit Logging: All system access and data interactions are logged and monitored.
- Testing: Continuous vulnerability scanning and regular independent penetration testing.
- Hardening: Shielded environments with least privileges administrator access.

5. Customer Data Ownership

- Healthcare organisations remain the sole owners of all health and personal data stored in MediMap.
- MediMap processes data only on behalf of the customer and does not sell, repurpose, or claim ownership of resident information.

6. Breach Response & Transparency

- NZ: Notifiable breaches are reported to the Office of the Privacy Commissioner.
- AU: Breaches are reported under the OAIC Notifiable Data Breaches scheme within 30 days.
- Impacted customers and individuals are notified promptly in line with regulatory requirements.

7. Customer Assurance

Customers may request:

- Backup verification reports
- Security audit logs
- Compliance attestations

MediMap is committed to transparency, compliance, and continuous improvement in protecting healthcare data.