Software Privacy Policy

Document Name	MediMap Software Privacy 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

MediMap is a digital medication management system designed to enhance safety, efficiency, and accuracy within aged care facilities and healthcare organisations in New Zealand and Australia. MediMap processes and stores health data, including patient medication records, to support healthcare delivery.

This Privacy Policy explains how MediMap complies with:

- New Zealand: Privacy Act 2020 and the Health Information Privacy Code 2020.
- Australia: Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), and the My Health Records Act 2012.
- State and Territory health privacy legislation in Australia, where applicable.

MediMap operates as a Software-as-a-Service (SaaS) provider. Healthcare organisations remain the data owners/controllers. MediMap acts as a data processor on their behalf.

1. Purpose and Scope

This Privacy Policy sets out how MediMap:

- Collects, uses, and protects personal information, including health data.
- Complies with AU/NZ privacy and health data laws.
- Defines responsibilities of healthcare organisations (data owners) and MediMap (data processor).
- Ensures transparency, accountability, and protection of sensitive health information.

2. Data Ownership and Processing

Data Owners:

Healthcare organisations such as aged care facilities, pharmacies, and prescribers that collect and use patient data.

Data Processor (MediMap):

- Stores and processes data only as instructed by the data owner.
- Implements security and compliance measures.

Software Privacy Policy

- Does not sell, repurpose, or assume ownership of patient data.

3. Personal Information Collected

Category	Examples	Purpose
Personal Identification	Name, DOB, gender, patient ID	Patient identification and care management
Health Information	Medical history, medication details	Safe medication administration
Medication Administration	Dose, time, route, logs	Medication tracking and compliance
Pharmacy & Prescriber Data	Prescriber names, pharmacy details	Prescription management
User & Access Data	Login details, audit logs, roles	Security and accountability

4. Legal Basis for Processing

MediMap complies with:

- NZ: Privacy Act 2020 and Health Information Privacy Code 2020 (including the 12 Rules governing collection, storage, access, correction, use, and disclosure of health information).
- AU: Privacy Act 1988, APPs, My Health Records Act 2012, plus relevant State/Territory laws (NSW HRIP Act 2002, VIC Health Records Act 2001, QLD Information Privacy Act 2009, etc.).

5. Third-Party Processors

MediMap uses selected third-party service providers (e.g. cloud hosting, analytics, penetration testing firms). These providers:

- Are subject to strict contractual terms, including confidentiality and data protection obligations.
- May only process data as necessary to deliver the contracted services.
- Are vetted through risk assessment and compliance checks before engagement.
- A current list of key sub-processors is available on request.

6. Cross-Border Data Transfers

- Data for NZ customers is hosted and backed up exclusively in Australia.
- Data for AU customers is hosted and backed up exclusively in Australia.

- Health data is not transferred offshore.
- Any exception (e.g. if a customer requests an offshore transfer) requires explicit written consent and assurance of equivalent legal protections.

7. Data Retention and Deletion

Data Type	Retention Period	Justification
Patient Health Records	7 years minimum, or until age 25	NZ & AU law compliance
Medication Administration	7 years minimum	Clinical audit & compliance
Prescriber/Pharmacy Records	7 years minimum	Regulatory compliance
Audit Logs & Access Records	As long as required	Security & accountability

Deletion Policy:

- After retention requirements, data is securely archived, then permanently deleted using industry-standard protocols.
- Deletion logs are maintained for audit trail purposes.

8. Data Access and Security

Access Control: Role-based access (nurse, prescriber, pharmacist).

Security Measures:

- Encryption in transit (TLS 1.2+) and at rest (AES-256).
- Multi-factor authentication (MFA).
- Full audit logging of access and modifications.
- Regular vulnerability scanning and penetration testing by accredited third parties.
- Disaster recovery tested against defined RPO/RTO targets.

Framework Alignment:

MediMap aligns with ISO/IEC 27001 information security management principles and the Australian Cyber Security Centre's Essential Eight maturity model.

9. Rights of Individuals

Individuals have rights under NZ and AU privacy law, including to:

- Access their personal information.
- Request correction of inaccurate or incomplete records.
- Request details of how their data is used or shared.
- Complain to:
    - The NZ Privacy Commissioner (for NZ residents).
    - The OAIC or relevant State/Territory body (for AU residents).

10. Breach Notification

If a privacy breach occurs:

1. Contain and secure systems.
2. Assess the nature and extent.
3. Notify affected individuals and regulators (NZ Privacy Commissioner or OAIC) as required.
    - AU: within 30 days under the Notifiable Data Breaches scheme.
4. Implement corrective measures.
5. Document the breach and response.

11. End-of-Contract Data Management

- Deactivation: Access revoked immediately; data archived securely.
- Data Extraction: Provided on request to the data owner in a structured, secure format.
- Deletion: Following confirmation of transfer, data is securely and permanently deleted.

12. Contact

Questions, comments, or privacy requests should be directed to:

Email: support@medimap.health