SECURITY WHITEPAPER

Your Patients' Data, Protected at Every Step

A comprehensive overview of how Medflow protects sensitive patient information through industry-leading security measures, compliance frameworks, and Australian data sovereignty.

Medflow Solutions Pty Ltd

Sydney, Australia

January 2026

Executive Summary

We understand that trusting a platform with patient information is a significant decision. Medflow was built from the ground up with healthcare security requirements at its core. This whitepaper details our comprehensive approach to protecting your patients' data across every touchpoint in our system.

As a medical practice management solution designed specifically for Australian specialist physicians, Medflow implements multiple layers of security controls that meet or exceed the requirements of SOC 2 Type II, HIPAA, ISO 27001, and the Australian Privacy Act. Our architecture ensures that sensitive patient data never leaves Australian jurisdiction while maintaining the highest standards of encryption, access control, and audit capability.

Compliance Certifications

SOC 2 Type II Certified	**HIPAA** Compliant	**ISO 27001** Certified

Security Features

1. Bank-Grade Encryption

All data processed by Medflow is protected using AES-256 encryption, the same standard used by financial institutions worldwide to protect sensitive transactions. This applies to data both in transit and at rest.

Data in Transit:

- All communications use TLS 1.3, the latest and most secure transport layer protocol
- Certificate pinning prevents man-in-the-middle attacks
- HTTP Strict Transport Security (HSTS) enforced across all endpoints
- Perfect Forward Secrecy ensures past communications remain secure even if keys are compromised

Data at Rest:

- Database encryption using AES-256 with per-tenant encryption keys
- Encrypted backups with geographically separated storage within Australia
- Secure key management with automatic key rotation
- File storage encryption for all uploaded documents and generated PDFs

2. Australian Data Residency

Your patients' data never leaves Australia. Medflow's infrastructure is hosted entirely on Australian servers, ensuring full compliance with Australian privacy legislation and data sovereignty requirements.

Infrastructure Details:

- Primary hosting in Sydney (ap-southeast-2) data centres
- Disaster recovery site in Melbourne for business continuity
- No data replication to overseas regions under any circumstances
- Edge caching disabled for patient data to ensure residency compliance
- Data centres certified to ISO 27001, SOC 1, SOC 2, and PCI DSS standards

3. PBS Integration Approved

Medflow maintains direct, sanctioned integration with PBS (Pharmaceutical Benefits Scheme) systems. This official integration means no workarounds, no grey areas, and complete compliance with PBS authority requirements.

Integration Capabilities:

- Official PBS form templates maintained and updated in accordance with Services Australia requirements
- Automated workflow management for authority prescriptions
- Digital submission pathways that meet regulatory standards
- Complete audit trail for all PBS-related activities

4. Privacy Act Compliant

Medflow operates in full compliance with the Australian Privacy Principles (APPs) under the Privacy Act 1988, as well as healthcare-specific privacy requirements including state health records legislation.

Privacy Controls:

- Data minimisation principles applied throughout the platform
- Clear consent management for patient data collection and use
- Right to access and correction functionality built into the platform
- Data retention policies aligned with medical record keeping requirements
- Privacy impact assessments conducted for all new features

5. Role-Based Access Control

Control exactly who in your practice can view and submit authorities. Medflow provides complete access management through a comprehensive role-based security model that ensures staff only access the data and functions necessary for their role.

Available Roles:

Role	Permissions
Doctor	Full access to patient records, authority submissions, and prescribing functions
Nurse	Patient data entry, form preparation, limited view access
Admin	Practice management, user administration, audit log access

Access Control Features:

- Multi-clinic support with isolated data environments
- Row-Level Security (RLS) enforced at the database level
- Session timeout and automatic logout for inactive users
- Audit logging of all access and permission changes

6. Regular Security Audits

Independent security assessments ensure our protections stay current with evolving threats. Medflow engages third-party security specialists to conduct regular penetration testing and vulnerability assessments.

Security Assessment Program:

- Annual third-party penetration testing by certified ethical hackers
- Quarterly vulnerability scanning and remediation cycles
- Continuous automated security monitoring and alerting
- Code security reviews integrated into development workflow
- Dependency vulnerability scanning with automated updates

Technical Architecture

Medflow is built on a modern, security-first architecture that leverages industry-leading technologies and best practices.

Infrastructure

- Deployed on Vercel's enterprise-grade hosting platform
- Database hosted on Supabase (PostgreSQL) with Australian region deployment
- Edge functions for serverless compute with minimal attack surface
- Automatic scaling and DDoS protection included

Authentication & Identity

- Supabase Auth with secure session management
- Support for multi-factor authentication (MFA)
- Password policies enforcing complexity requirements
- Brute force protection with account lockout

Data Isolation

- Multi-tenancy model with strict clinic-level data separation
- Row-Level Security (RLS) policies enforced at database level
- SECURITY DEFINER functions for secure cross-table queries
- No possibility of data leakage between practices

Incident Response

Medflow maintains a comprehensive incident response plan to address any security events quickly and effectively.

Response Capabilities:

- 24/7 security monitoring and alerting
- Documented incident response procedures aligned with ISO 27001
- Breach notification procedures compliant with Notifiable Data Breaches scheme
- Regular incident response drills and tabletop exercises
- Post-incident review and continuous improvement process

Business Continuity

Medflow implements robust business continuity measures to ensure your practice operations are never interrupted.

- 99.9% uptime SLA with redundant infrastructure
- Automated daily backups with point-in-time recovery
- Geographically distributed backup storage within Australia
- Disaster recovery plan with 4-hour RTO (Recovery Time Objective)
- Annual disaster recovery testing and validation

Conclusion

At Medflow, we understand that security is not just a feature—it's a fundamental requirement for any system handling patient health information. Our comprehensive security framework, combined with our commitment to Australian data residency and regulatory compliance, ensures that your patients' data receives the protection it deserves.

We continuously invest in improving our security posture and welcome any questions about our practices. For additional information or to discuss your specific security requirements, please contact our team.

Contact Information

Medflow Solutions Pty Ltd

Website: clinic.medflow.com.au
Email: admin@medflow.com.au
Location: Sydney, Australia