# Consultmed Security Overview

*Consultmed is a secure, Australian hosted Software as a Service platform for managing digital referrals, Advice & Guidance, and other clinical correspondence.*

*Our security programme aligns with recognised industry standards, including ISO IEC 27001 principles and the Australian Privacy Principles. We use a defence in depth approach, with secure Microsoft Azure hosting within Australia, strong encryption, and enforced multi factor authentication. This is supported by continuous monitoring, regular security audits, penetration testing, and a documented incident response framework.*


**1. Where is data hosted and how is it protected?**

All Consultmed data is hosted exclusively within Microsoft Azure Australian data centres. The primary production environment is located in Sydney Australia East, with a secondary geo redundant environment in Melbourne Australia Southeast.

Data is encrypted in transit using TLS version 1.2 or higher and encrypted at rest using AES 256 encryption. Security monitoring and threat detection are provided through Microsoft's integrated cloud security capabilities, supported by layered access controls, network security rules, and strict authorisation safeguards designed to prevent unauthorised access.

**2. How do users access the platform securely?**

Access to Consultmed is governed by role based permissions and enforced multi factor authentication for all users.

# Consultmed Security Overview

The platform supports enterprise identity integration via Microsoft Entra ID and Active Directory Federation Services. Multi factor authentication is enforced either through the customer's identity provider or directly within Consultmed, depending on the deployment model.

Strong password policies apply, including minimum length and complexity requirements, along with automatic account lockout after repeated failed authentication attempts.

Consultmed does not store or access plaintext passwords. Authentication is handled through industry standard identity services, including Okta Auth0 or the customer's own identity platform.

**3. What security standards and governance does Consultmed follow?**

Consultmed's information security framework aligns with recognised industry standards and best practice, including ISO IEC 27001, the Australian Privacy Principles, and the Australian Cyber Security Centre Essential Eight.

The Consultmed platform is hosted on Microsoft Azure, which is independently certified against ISO IEC 27001, ISO IEC 27017 for cloud security, ISO IEC 27018 for protection of personal data in the cloud, SOC 2, and IRAP. Consultmed's internal controls and operational practices build on these certified foundations to meet enterprise and healthcare security expectations.

Governance measures include role based access control, enforced multi factor authentication, encryption, centralised monitoring, regular security audits, penetration testing, and formal incident response and escalation processes.

**4. How are threats, vulnerabilities, and software quality managed?**

System activity and security events are logged and monitored centrally using Microsoft's cloud security and monitoring capabilities. Continuous vulnerability scanning, regular security reviews, and independent third party penetration testing are performed to identify and address risks proactively.

# Consultmed Security Overview

We conduct regular security audits to identify potential vulnerabilities and address them early. Secure software development practices are embedded across the development lifecycle, including automated testing, peer code review, regression testing, and structured user acceptance testing.

Our security and engineering teams actively monitor emerging cyber security threats and apply security patches and platform updates promptly, ensuring Consultmed remains protected against current and emerging risks.

**Users**
User access, activity, and behaviour are monitored to detect anomalous patterns. Combined with enforced multi factor authentication and role based permissions, this helps protect user accounts and sensitive clinical information.

**5. How is client data segregated in a shared cloud environment?**

Consultmed operates a secure multi tenant architecture with strict logical segregation between customers.

Each client's data is isolated at the application and database layers using unique organisational identifiers, separate encryption keys, and network segmentation through Azure Virtual Networks and Network Security Groups. Access is restricted by role and organisation, with multi factor authentication enforced across all access paths. Optional IP allowlisting can be enabled where required.

**6. How are data backup, disaster recovery, and business continuity managed?**

Encrypted backups are performed automatically on a daily basis and retained in line with defined backup and retention policies. Backups are stored across geographically separate Azure regions in Sydney and Melbourne to protect against data loss or regional outages.

Consultmed maintains a documented disaster recovery and business continuity plan that defines recovery time objectives and recovery point objectives, supported by clear response procedures. These plans are reviewed and tested on a regular basis.

# Consultmed Security Overview

As a cloud native organisation, Consultmed can maintain operational continuity even if physical offices or local infrastructure are unavailable.

**7. How does Consultmed protect email communication from spoofing?**

Consultmed protects outbound email using DMARC, SPF, and DKIM controls.

These mechanisms verify that messages originate from authorised sources and include valid cryptographic signatures. Unauthorised or suspicious messages are automatically rejected or quarantined, with monitoring and reporting in place to detect and prevent phishing or spoofing activity.

**Privacy, terms, and transparency**

Consultmed is committed to transparency in how personal and health information is handled.

Our **Privacy Policy** outlines how we collect, use, store, and protect personal information in accordance with applicable privacy laws and recognised best practice.

Our **Terms and Conditions** describe the contractual, operational, and security obligations that apply to use of the Consultmed platform.

- Privacy Policy: https://www.consultmed.co/privacypolicy
- Terms and Conditions: https://www.consultmed.co/terms-of-service/

These documents are reviewed regularly and form part of Consultmed's broader governance and assurance framework.