



Allied Health

Secure, compliant IT infrastructure
for healthcare environments

CMTG.COM.AU



The Reality of IT in This Sector

Allied health practices manage some of the most sensitive data in any sector.

Patient records, clinical notes, imaging files, referral pathways, and Medicare compliance obligations create an IT environment where security, reliability, and data residency are not optional considerations. They are professional and regulatory obligations. A practice that cannot access its clinical systems during operating hours, or that experiences a data breach affecting patient records, faces consequences that go well beyond an IT inconvenience.

The Pressure Points

- Patient data is subject to the Privacy Act and the Australian Privacy Principles, with specific obligations around storage, access, and breach notification
- Clinical software platforms including practice management systems and imaging tools require consistent, low-latency compute to perform reliably across multiple practitioners and locations
- Multi-site practices need secure, fast connectivity between locations without the complexity of managing network infrastructure internally
- Ransomware targeting healthcare is escalating globally. A compromised practice management system during operating hours directly affects patient care
- Staff are not IT professionals and need an environment that simply works, with support available when it does not
- Growing practices adding practitioners, locations, or services need IT infrastructure that scales without a major capital investment each time

Why Standard IT Falls Short

General-purpose MSPs provide support and backup services but rarely understand the specific compliance obligations of a healthcare environment or the clinical software stack well enough to manage it proactively.

Public cloud platforms introduce data residency questions that most practices cannot answer clearly when asked by a privacy regulator. The combination of clinical compliance knowledge, sovereign infrastructure, and genuine 24/7 monitoring is uncommon in the WA market. continuity issue.

What CMTG Brings to This Sector

1



SOVEREIGN, COMPLIANT DATA STORAGE:

Patient data hosted on CMTG's private cloud platform stays in Western Australia on infrastructure CMTG owns. No exposure to foreign jurisdiction risk. A clear, auditable answer to where patient data lives and who can access it.

2



PRACTICE-LEVEL RELIABILITY:

Proactive NOC monitoring and 99.9% uptime commitment means clinical systems are available when practitioners need them. Issues are identified and resolved before they affect patient-facing operations.

3



IMMUTABLE BACKUP AND RAPID RECOVERY:

In the event of a ransomware incident or system failure, CMTG's immutable backup architecture enables recovery to a known-clean state within the hour. Patient data is protected and the practice is back operating quickly.

4



SCALABLE INFRASTRUCTURE FOR GROWING PRACTICES:

Whether a practice is adding a new location, bringing on additional practitioners, or moving to a multi-disciplinary model, CMTG's cloud infrastructure scales to match without requiring hardware investment.



What It Looks Like in Practice

A multi-site allied health group across the Perth metropolitan area migrated from a combination of on-premises servers and a consumer-grade cloud backup service to CMTG's sovereign cloud platform.

CMTG implemented a managed IT agreement covering all locations, deployed Fortinet endpoint protection across all devices, and established immutable backup of the practice management system and clinical records. The practice now has a single IT partner managing the full environment, a clear answer to where patient data lives, and DR testing conducted quarterly.

Relevant Credentials

1



PRIVACY COMPLIANCE:

Sovereign WA infrastructure with full audit trail, supporting Australian Privacy Principle obligations

2



CYBER SECURITY:

Fortinet Advanced Partner with full EDR, SOC, and endpoint protection capability

3



RECOVERY:

Sub-1-hour RTO and application-aware immutable backup via IBM Safeguarded Copy

4



LOCAL SUPPORT:

Perth-based team with 36 technical specialists and a dedicated Technical Account Manager

If your practice has questions about where patient data is stored, whether your current backup would actually survive a ransomware incident, or how to demonstrate compliance with your data obligations, a conversation with CMTG is a practical starting point.