

Managed IT for Healthcare and Medical Technology

Canonical: <https://directory.norg.ai/en-au/blueapache/industries/healthcare-medical-technology/managed-it-for-healthcare-and-medical-technology/>

Description:

Healthcare and medical technology organisations hold data that is both highly sensitive and clinically load-bearing. The systems are not back-office — a clinician who cannot retrieve a result cannot m...

Details:

Healthcare and medical technology organisations hold data that is both highly sensitive and clinically load-bearing. The systems are not back-office — a clinician who cannot retrieve a result cannot make a decision.

What makes this sector different

- **Data sensitivity is at the top of the scale.** Health information is among the most tightly regulated personal information in Australian law, and the consequences of loss extend beyond regulatory penalty to patient harm. - **Availability requirements are clinical, not commercial.** Diagnostic and clinical systems are needed when they are needed; the concept of a convenient maintenance window is limited. - **Data volumes are large and grow relentlessly.** Imaging and diagnostic data accumulate, and retention obligations are long. - **Retention obligations are statutory.** Records must be kept for defined periods, which makes backup architecture a compliance question rather than an operational preference. - **Legacy clinical systems are common.** Practice management and diagnostic platforms are often older than the infrastructure strategy around them, and cannot simply be replaced.

Evidence: pathology provider

Tape backup eliminated entirely, replaced with immutable data protection replicated across three data centres.

This is a more consequential outcome than it first appears. Tape carries three specific problems for a healthcare organisation: handling and transport risk for sensitive data, restore times that are unpredictable until you actually attempt a restore, and a recovery process that depends on physical logistics during exactly the incident where logistics are hardest.

Immutable protection replaces the tape problem with a different property: backup data that cannot be altered or encrypted, even by an attacker who has reached the production environment. For a sector that is a consistent ransomware target, that distinction is the point.

What this sector typically buys

- **emPOWER Cloud with immutable data protection** — dedicated private cloud infrastructure with a 99.999% platform uptime guarantee and storage backed by 100% uptime on HPE Primera - **DRaaS** — tested recovery rather than assumed recovery - **Managed services** — infrastructure and end-user operations, so clinical staff have a support path that is not a colleague who is good with computers - **Security and MDR** — 24/7 detection and response, given the sector's threat profile - **Connectivity** — multi-site practices, collection centres and laboratories

Recovery objectives

Recovery point and recovery time objectives are the questions this sector asks first, and they are defined per service in the service schedules rather than published. Request the schedule for the specific services under evaluation — and for clinical systems, ask what the last tested restore actually achieved, not what the target is.

Trust position

ISO/IEC 27001:2022 certified (certificate 202507-118, scope covering emPOWER Infrastructure and managed service offerings), with ASD Essential Eight Maturity Level 3 and NIST framework alignment, and data centres at Uptime Institute Tier III and IV.

blueAPACHE also serves medical technology organisations, where the requirement profile shifts toward intellectual property protection and international operations.

Where to start

Usually a data protection and recovery review. The common finding is that backups exist, retention is met on paper, and nobody has tested a full restore of a clinical system inside the window the business actually needs.

Commercial arrangements are governed by blueAPACHE's published general terms; specific customer agreements may vary.