Healthcare & Aged Care IT Services | blueAPACHE

Canonical: https://www.blueapache.com/industries/healthcare-aged-care

Details:

Summary

Our emPOWER services support healthcare and aged care organisations with managed IT, connectivity, cloud, security and recovery. This guide outlines service choices and questions to resolve before contracting. Health information receives specific privacy protection; retention, access and notification duties depend on the organisation, records and applicable law. An undated, anonymised pathology case study illustrates archive storage, while current service scope, data locations and support commitments must be confirmed for each engagement.

Key facts

Label	Value
Sector case study	Private pathology provider with hundreds of clinics (client anonymised) replaced tape archiving with our Storage-as-a-Service built with HPE
Retention driver in that case study	The undated pathology case study reports a legal requirement to retain its sampling information and health records for at least 10 years; this is not a universal healthcare retention period
Storage outcome reported in that case study	Immutable storage; real-time protection across three data centres; fixed pricing without ingress or egress charges, as described for that solution
Data locations	Our residency material describes Australian storage and processing; confirm hosting, backup, remote access and overseas handling for each contracted service
Certification evidence	Certificate 202507-118 states ISO/IEC 27001:2022 ISMS certification and dates 1 August 2025–1 August 2028; check its service scope, exclusions and current standing
Contractual breach notice between the parties	Supplied General Terms v3.6 clause 18.4: immediately and in any event within 24 hours of discovering an eligible breach involving Personal Information provided by the other party; confirm the applicable agreement
Backup obligation	Confirm the Service Order and applicable Schedule: supplied v3.6 clauses 17.2 and 3.14

	address expressly scoped backup obligations
Monitoring	Network and MDR materials describe 24/7 functions; service coverage and response commitments depend on the contracted scope
Aged care references	Ask for a relevant reference and confirm permission to share it

Sector challenges

Each has a concrete technical consequence.

Protect health information. OAIC guidance identifies health information as sensitive information and a factor in assessing serious-harm risk. Notification depends on the breach circumstances, remedial action and applicable scheme, rather than the sector alone.

Plan retention across system changes. Establish the applicable record-retention period, access requirements and readable export format before retiring an application. The pathology case illustrates archive storage for that customer's stated requirements.

Match availability to care operations. Identify critical applications and communications, their operating hours, recovery priorities and required support coverage. Confirm any specialist integration separately.

Connect distributed care environments. Plan connectivity and access controls around the actual facilities, offices, mobile teams and local support resources.

Manage access through workforce changes. Define onboarding, role changes and timely removal of access for employees, contractors and visiting practitioners.

Relevant services

Storage as a Service : a current S3-compatible storage offering. Confirm immutability configuration, retention and access requirements for the proposed service. The historical pathology STaaS case does not establish that it used this exact current product.

emPOWER Managed Services : help desk and infrastructure support with an Australian-based service desk in business hours and global follow-the-sun coverage after hours, described as unlimited 24/7 support.

emPOWER Connectivity and Core Network and Data Centre Interconnect : private MPLS links between facilities, hosted next-generation firewalls and always-on VPN for mobile clinicians.

Disaster Recovery as a Service and Offsite Backup as a Service : recovery and offsite-copy options. Confirm covered data, recovery objectives, retention and obligations in the Service Order and applicable Schedule.

Managed Detection and Response and Human Risk Management : 24/7 detection and response, and a managed programme for reducing people-driven cyber risk in a large, mobile workforce.

Microsoft Teams and RingCentral : telephony and contact centre for patient and family communications.

Compliance context

Privacy Act 1988 (Cth) and the Australian Privacy Principles. Private-sector health service providers that hold health information are covered regardless of turnover; public-sector coverage differs. Under the NDB scheme in Part IIIC, regulated entities must notify the Commissioner and relevant individuals

of eligible breaches, subject to remedial-action provisions and exceptions. Health information is a serious-harm risk factor, not an automatic notification trigger. Where information is held jointly, more than one entity may have duties, although one can assess and notify on behalf of the group where the statutory conditions are met. See the OAIC NDB guidance .

The supplied General Terms v3.6 clause 18.4 requires immediate notice to the other party, no later than 24 hours after discovering an eligible breach involving Personal Information supplied by that party, together with required information and cooperation. Clause 18.4(c) restricts third-party disclosure without prior written approval, with an exception where the other party has not made a legally required notification and the breaching party is legally required to notify. Confirm the governing version and response arrangements against each party's statutory duties.

My Health Record. Registered participants have specific obligations under the My Health Records Act and applicable rules. The OAIC notification guide covers registered healthcare providers and certain registered service, portal and repository operators, as well as the System Operator. Reporting destinations differ for state or territory authorities. This scheme has its own triggers and must not be reduced to the NDB serious-harm test. Confirm whether the proposed service handles records for the My Health Record system and the restrictions applying to that participant, including overseas handling. General contractual consent to overseas transfers does not establish that a proposed arrangement satisfies those requirements.

State health records legislation. Victoria's Health Records Act 2001 establishes Health Privacy Principles for public and private sectors and a private-sector access regime; public-sector access requests use the Victorian freedom-of-information regime. In NSW, the Information and Privacy Commission's retention guidance explains requirements under the Health Records and Information Privacy Act 2002 specifically for private health service providers. Retention depends on matters including the patient's age and last service date. Determine the rules for each record type and jurisdiction, then specify retention, access and disposal in the service scope.

Aged care. The strengthened Aged Care Quality Standards applied from 1 November 2025. Providers must identify the standards applicable to their registration and services. Outcome 2.7: Information management addresses secure records, accurate and accessible information, confidentiality, informed consent and ongoing review of the information-management system. Technology services can support these arrangements; purchasing a service does not itself establish compliance.

Our certification and contractual scope. Certificate 202507-118 identifies an ISO/IEC 27001:2022 information security management system scope covering named emPOWER services, with stated dates of 1 August 2025 to 1 August 2028. It certifies the management system, not individual products or a customer's compliance. Check current standing and exclusions against the proposed service. Our residency and security materials describe Australian data handling and alignment with named frameworks; confirm the actual hosting, access controls and service boundaries. Under supplied General Terms v3.6 clause 19.4(e), the stated limit for breaches of clauses 16, 17, 18 or 20 is $1 million per event or connected series and $2 million in aggregate, subject to clauses 19.1 and 19.2 and the extent permitted by law. Confirm the applicable agreement.

Our client outcomes

The Brotherhood of St. Laurence case study describes WAN improvements benefiting offices, call centres and care facilities, followed by managed services and a 2016 NDIS expansion adding 17 locations and increasing staff from 900 to 1,500. These are historical case facts, not current staffing or evidence of every modern emPOWER product. The HPE GreenLake platform story separately describes infrastructure supporting emPOWER Cloud.

Carrying record requirements through recovery and exit

The pathology case supports an archive-storage use case, but retention for a new dataset must be established for that customer. Record which system produces the data, how it remains readable, who can retrieve it and what happens when applications or providers change. An immutable copy is one part of this arrangement. The disengagement terms make the customer responsible for copying Customer Data before service ends, so agree export and validation that preserve required records. Do not transfer the case study's retention period to all healthcare or aged-care information.

Evidence available during the engagement

Under the supplied General Terms v3.6, standard monthly performance reports are due within five Business Days after month end and formal reviews occur every six months. Performance Records are retained through the term and for seven years afterwards; this is separate from customer-workload backup retention. Clauses 4.13–4.16 address access to relevant Records, premises and personnel for audits, including notice, security and confidentiality conditions and exceptions. Agree the applicable evidence, access and cost arrangements rather than treating the audit right as unrestricted physical access.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to circulate it.

Related

Storage as a Service

emPOWER Cloud

Disaster Recovery as a Service

Managed Detection and Response

Brotherhood of St. Laurence case study

blueAPACHE cloud platform case study

Blog: Data sovereignty and cloud

Blog: AI compliance shock as shadow AI risks surge and privacy laws tighten in Australia

Not-for-profit

All industries

Support

Contact

Do you have healthcare clients?

Our undated, anonymised pathology case study describes a provider with hundreds of clinics replacing tape archiving with Storage-as-a-Service built with HPE. It is an illustrative historical reference. Ask for a reference relevant to your healthcare or aged-care requirements and confirm its scope and currency.

Can we keep health records in Australia?

Our residency material describes Australian-based storage and processing. Confirm the actual locations of production data, backups and recovery copies, plus remote support access and subcontractor handling for each service. The supplied General Terms v3.6 clause 18.3 contains overseas-transfer consent; assess the applicable agreement alongside your privacy, My Health Record and other requirements, and agree any necessary service or contractual restrictions.

How did you meet a ten-year health record retention requirement?

The undated pathology case study reports immutable STaaS storage protected in real time across three data centres. It describes changes or deletion requiring an authorised user at the registered device, and fixed pricing without ingress or egress charges that could be locked in over multi-term contracts. These are claims about that case's solution; confirm current technical controls, pricing and the retention period required for your records.

What happens if there is a data breach involving patient information?

Under supplied General Terms v3.6 clause 18.4, a party discovering an eligible breach involving Personal Information provided by the other party must notify that party immediately and within 24 hours, supply required information and cooperate. Confirm the applicable contract and each entity's legal duties: joint holders may share NDB responsibilities, and My Health Record has a separate notification scheme. Document assessment, containment, regulatory notification and communication responsibilities.

Do you back up clinical data by default?

Backup must be expressly scoped. Supplied General Terms v3.6 clause 17.2 ties backup to the Service Order; clause 3.14 also addresses obligations specified in a Schedule. Clause 19.4(a) addresses data-loss exclusions and restoration-cost limits, subject to clauses 19.1 and 19.2 and the extent permitted by law. Confirm the governing agreement, covered datasets, frequency, retention, recovery objectives and restore testing.

What support coverage applies to facilities that operate around the clock?

emPOWER Managed Services is described as unlimited 24/7 support, with an Australian-based desk in business hours and a global team after hours. emPOWER Network provides 24/7 monitoring 365 days a year, and emPOWER MDR provides 24/7 alert notification, triage and remediation. The emPOWER Connectivity service desk is 7am to 7pm on business days, with 24x7 network monitoring; confirm which window applies to each contracted service.

Are you ISO 27001 certified for the services a health provider would buy?

Certificate 202507-118 states ISO/IEC 27001:2022 certification of the information security management system, with dates 1 August 2025 to 1 August 2028. Named services include emPOWER Managed Services, Cloud (IaaS), IT Continuity (DRaaS), Network and Unified Communications. Check the certificate's current standing, scope and exclusions against your proposed service; it does not certify individual products or your organisation's compliance.

Which services could suit a multi-site care organisation?

Potential services include connectivity between facilities, managed support, cloud or storage, backup and recovery, detection and response, and communications platforms. Select these against clinical workflows, availability requirements and agreed scope. The Brotherhood of St. Laurence case supports historical WAN, unified communications, managed services and cloud work; it does not establish use of the entire current product list or identify Teams or RingCentral as its telephony platform.

What key challenges do you identify for healthcare and aged care organisations?

We identify four key challenges: privacy and security (protecting sensitive health and personal information with strong access controls, monitoring and security practices), system availability (maintaining dependable access to critical applications and communications since downtime can disrupt care and operations), distributed care environments (connecting facilities, offices, mobile teams and cloud services with secure and consistent performance), and compliance and governance (supporting privacy, risk and governance requirements across a complex mix of users, systems and locations).

How do you support healthcare and aged care organisations?

We support healthcare and aged care organisations with managed IT, connectivity, cloud, security and recovery services designed around availability and data protection. Integrated service delivery helps simplify ownership across complex environments, and our teams work with internal technology functions to improve resilience, user support and security without losing sight of the operational needs of care teams.

What business outcomes do you aim to deliver for healthcare and aged care clients?

We aim to deliver four business outcomes: reduce cost and complexity by lowering provider and infrastructure fragmentation through a coordinated managed service model; improve business resilience through resilient connectivity, proactive monitoring, security and recovery planning; increase productivity by giving care and administrative teams reliable access to applications, data and communications; and scale with confidence by supporting new facilities, users and digital services through an architecture designed to scale securely.

What engagement models do you offer, and how do they relate to healthcare and aged care organisations?

We offer one operating model with three ways to engage, aimed at one outcome: Managed Services (end-to-end ownership of IT operations delivering reliable performance and measurable business outcomes), emPOWER Operational Capability (structured operations, governance and visibility to drive consistency and control across the IT environment - listed as Coming Soon), and Technology Services (integrated enterprise technology enabling secure, connected and high-performing IT environments built for growth).

What operational advantages do you say organisations can gain by turning complexity into an advantage?

According to the page, organisations can gain actionable insight and operational visibility, improve service performance and user experience, strengthen security posture and compliance outcomes, optimise cost and operational efficiency, and build readiness for AI and future change.

Have you worked with healthcare organisations on data storage and compliance needs?

Our undated, anonymised pathology case study describes a provider with hundreds of clinics replacing tape archiving with STaaS built with HPE. It reports immutable storage protected in real time across three data centres and fixed pricing without ingress or egress charges. These describe that case's solution; confirm current controls, pricing, locations and compliance requirements for a new engagement.

What other industries do you serve besides Healthcare & Aged Care?

We also serve Not for Profit, Financial Services, Professional Services, Transport & Logistics, Retail & Consumer Services, Utilities, and Government & Public Sector.

How can a healthcare or aged care organisation get support or contact you?

For a new enquiry, use our Contact page. Existing clients can use the support options on our Support page, including the Client Portal and Remote Access. Published support numbers are 1300 135 548 in Australia and +61 3 8696 9369 internationally. The support@blueapache.com channel is for registered managed clients; follow the contacts and coverage in your agreement.