

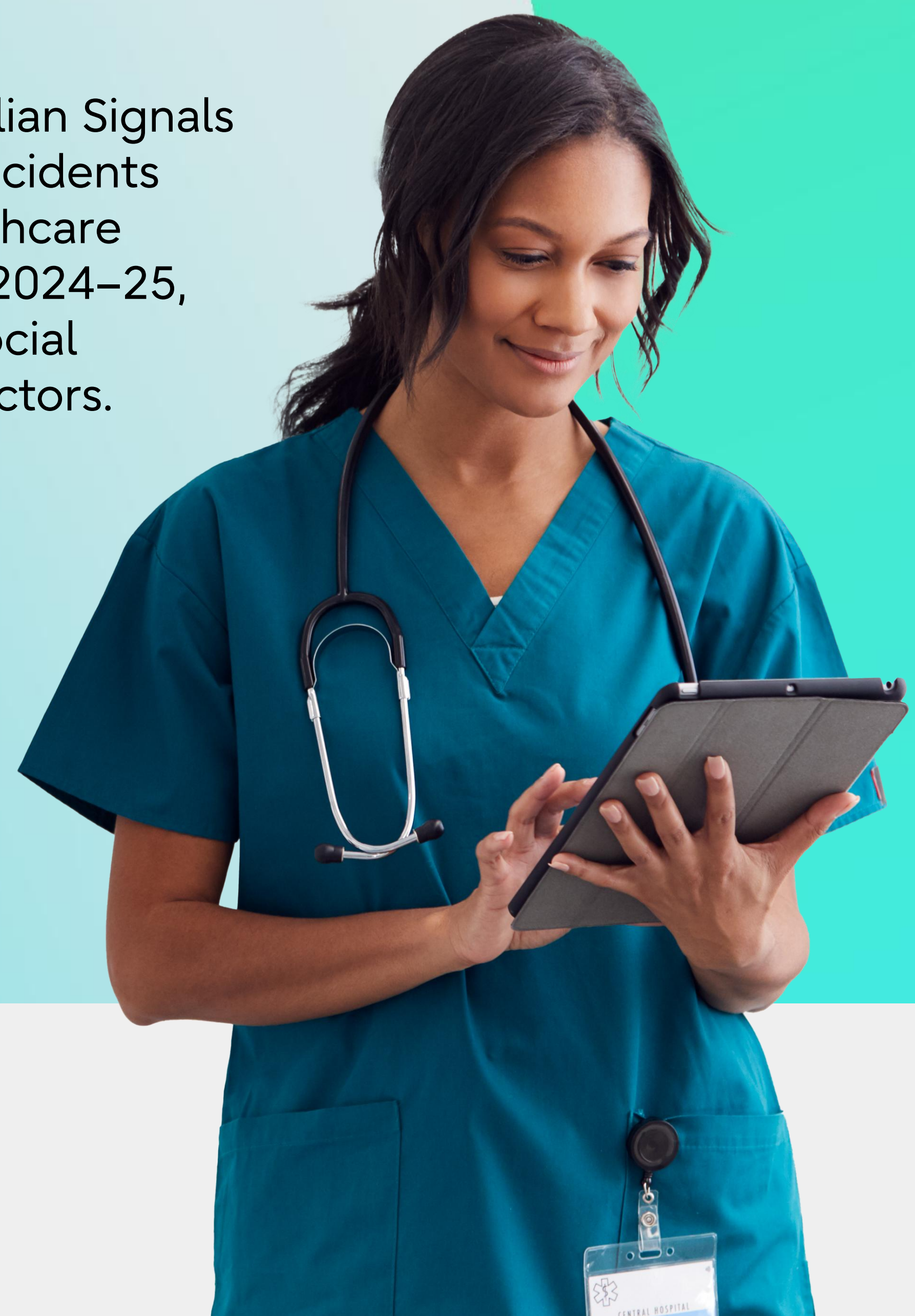
Safeguarding digital care: Clinically safe cloud strategies for Australia's health leaders



Today, healthcare is increasingly digital, with technology now integral to care delivery. Many healthcare organisations rely on Digital Health Record (DHR) or Electronic Medical Record (EMR) platforms as core clinical systems. When these platforms go down, hospitals can quickly grind to a halt and patient safety is put at risk.

The cyber threat is also intensifying. According to the Australian Signals Directorate's Australian Cyber Security Centre, cybercrime incidents against the Australian healthcare sector are increasing. Healthcare organisations remain attractive and vulnerable targets: in FY2024–25, malicious actors were successful in 95% of healthcare and social assistance sector incidents, compared with 52% across all sectors.

At Fujitsu, we understand that clinical information systems are critical to care quality, continuity and trust. As DHR and EMR workloads move to public cloud, healthcare providers need a partner that can deliver performance, uptime and business continuity through a managed service that is cyber-resilient, clinically safe and economically sustainable.



From “Where do we host?” to “How do we operate safely?”

Traditional infrastructure conversations focus on platforms: which cloud, which hypervisor, which storage. In healthcare, that is the wrong starting point.

For EMR and other sensitive workloads, the real questions are:

- How do we guarantee clinical safety and availability when infrastructure fails?
- How do we protect highly sensitive patient data against increasingly sophisticated cyber threats?
- How do we simplify a complex vendor landscape, so accountability is clear when something goes wrong?
- How do we maintain sovereignty, compliance and trust while still innovating with cloud, AI and data?
- How do we ensure clinician experience is improved, not degraded, by new platforms and controls?

Fujitsu's position is clear: the hosting model should be shaped by health outcomes, risk and clinician experience, not by a single vendor or technology choice.

This means:

- Cloud native, not infrastructure led:** platforms that can evolve continuously, not static “lift and shift” environments.
- Outcomes based, end to end services:** a single accountable partner across infrastructure, security, operations and clinical service levels.
- Security embedded by design:** Zero Trust principles, continuous monitoring and automated response, not bolt on controls.



The reality: EMR estates built on yesterday's assumptions

Across government health and large providers, we see a consistent pattern when we assess EMR and clinical hosting environments:

Over provisioned, under utilised infrastructure

Capacity was sized “just in case” to avoid clinical outages. CPU utilisation at 20–30% and memory at 50–60% is common. Under older commercial models this was tolerated. Under modern subscription and core-based pricing, it becomes structural cost and risk.

Fragmented contracts and unclear accountability

EMR hosting is often surrounded by a constellation of small contracts – networking, storage, monitoring, backup, cyber, integration, service desk. When an incident occurs, accountability is blurred and resolution is slow. No one owns the end-to-end clinical outcome.

Sensitive data spread across the estate

Clinical documents, images and personally identifiable information (PII) often sit on general purpose file shares, legacy systems or poorly governed data stores. The EMR may be secure; the surrounding ecosystem is not. This undermines both compliance and interoperability ambitions.

Legacy operating models in a cloud world

Many EMR platforms were lifted into hosted or cloud environments without rethinking the operating model. Processes, roles and controls still assume a static data centre, not a dynamic hybrid cloud with automation, AIOps and continuous change.

These are not technology failures. They are the result of years of incremental change without periodically stepping back and asking: **Does this still make sense for our clinical risk, cyber posture, clinician experience and budget?**

What's needed now is platform evolution – not just a new hosting contract, but a managed service that embeds continuous optimisation, security and data driven decision making.



Why healthcare needs a different cloud conversation

Healthcare is not just another regulated industry.

EMR and clinical systems carry a unique combination of:

- **High value data**
Rich longitudinal patient records, diagnostics, images and notes.
- **High regulatory and public scrutiny**
Privacy, consent, clinical safety standards and public trust.
- **High impact availability**
Downtime is not just an SLA breach; it is a patient safety issue.
- **High threat profile**
Ransomware operators know health organisations are more likely to pay and less able to tolerate disruption.

That combination means generic “move to cloud” narratives are insufficient.

Health organisations need:

- **De risked, controlled EMR and DHR transformation**
Structured transition and hybrid delivery that actively manages clinical and cyber risk.
- **Single point of accountability**
One partner responsible for end-to-end service outcomes across all layers, from infrastructure to clinician experience.
- **Security led, sovereign by design platforms**
Zero Trust, continuous monitoring and clear sovereignty controls built in from day one.
- **Data enabled platforms**
EMR and adjacent systems that unlock interoperability and insight, not just storage and compute.
- **Clinician centred operations**
Service levels, change windows and incident processes aligned to real clinical workflows.

Managing sensitive workloads under constant cyber threat

Fujitsu secures complex hybrid environments for thousands of customers globally, including government, critical infrastructure and regulated industries. The same principles apply – with even greater rigour – in healthcare.



For EMR and sensitive health workloads, we focus on:

End to end protection of infrastructure and data

From the data centre or cloud region through to the endpoint, we apply layered controls:

- Network segmentation and micro segmentation based on Zero Trust.
- Hardened platforms and secure configuration baselines.
- Encryption in transit and at rest for clinical and identity data.
- Secure backup, immutable storage and ransomware resilient recovery.

Compliance as a design input, not an afterthought

We work within recognised standards and regulatory frameworks across markets (for example ISO 27001/27017, health privacy regulations, and jurisdiction specific security frameworks). Compliance is:

- Embedded into architecture, patterns and operating procedures.
- Supported by transparent reporting, audit trails and governance dashboards.
- Continuously validated as platforms evolve – not re checked every few years.

Continuous threat detection, monitoring and response

Security is not a point in time activity. We provide:

- 24/7 monitoring across the EMR stack and surrounding systems.
- Advanced analytics and anomaly detection to spot early indicators of compromise.
- Automated playbooks and orchestrated response to reduce time to contain.

Operational resilience and tested recovery

We assume failure will happen. We design for:

- Graceful degradation and clinically safe fallback modes.
- Rapid failover across regions or sites for critical services.
- Regularly rehearsed recovery scenarios involving clinical teams, not just IT.

Identity, access and clinical context

Strong identity and access management ensures the right clinician has the right access at the right time – and only that. We:

- Integrate with clinical workflows and context (location, role, time, device).
- Apply least privilege and just in time access to reduce attack surface.
- Balance security with usability so controls support, not hinder, care delivery.

Cloud choice without clinical compromise

The cloud question in healthcare is no longer “public or private?” It is:

What is the right platform for each workload, given its clinical criticality, data sensitivity, interoperability needs and sovereignty requirements?

Fujitsu’s hybrid cloud approach is deliberately platform agnostic and outcome driven:

We support **private and sovereign cloud** for the most sensitive, latency-critical or jurisdiction-bound workloads.

We leverage **hyperscale public cloud** (Microsoft Azure, AWS and others) where it makes sense, for elasticity, analytics, AI and non-clinical workloads.

We enable **workload portability and modernisation** over time, so EMR and adjacent systems can evolve without wholesale “rip and replace”.

We apply a **consistent security and governance model** across environments, so policies, monitoring and controls follow the workload.

The principle is simple: **the right cloud for the right workload**, with a consistent operating model, security posture and clinician centred service experience across the estate.

From trend to practice: What a clinically safe cloud looks like

Continuous platform evolution

Regular, low risk change as part of a managed service, not disruptive, one off upgrades.

Single accountable provider

One partner responsible for availability, security, performance and clinician experience.

Security led architecture

Zero Trust, continuous monitoring and automated response embedded into the platform.

Data enabled EMR/DHR

Interoperable data services that support population health, research and AI, with strong privacy controls.

Low risk transition

Structured migration and hybrid operation, with clear guardrails around clinical risk and change windows.

Strong governance and sovereignty

Transparent controls for data residency, access, compliance and operational oversight.

Automation and AIOps

To reduce cost, minimise human error and improve service consistency.

Clinician experience as a core metric

Measuring success not just in uptime and cost, but in how well the platform supports care delivery.



How Fujitsu helps: Clinically safe cloud for EMR

Fujitsu brings together hybrid cloud, security, data and healthcare expertise into an integrated, outcomes-based service for EMR and sensitive health workloads.

Our approach delivers:

- **De risked, controlled EMR/DHR transformation**
Structured assessment, migration and modernisation aligned to clinical risk.
- **Single accountability for end-to-end outcomes**
From infrastructure and security through to service management and clinician SLAs.
- **Security led, sovereign by design platforms**
Built on Zero Trust, continuous monitoring and jurisdiction specific sovereignty controls.
- **Data driven, clinician focused outcomes**
Platforms that not only keep EMR running safely but unlock data for better decisions and better care.

For health organisations, the opportunity is clear: move beyond “where do we host?” to a clinically safe cloud model that is secure, sovereign, interoperable – and designed around the people who use it every day.

From cloud frenzy to right-sized hybrid cloud

Over the last five to ten years, many healthcare provider organisations moved enthusiastically to public cloud. The goal was understandable: reduce reliance on traditional data centres, avoid further expansion of on-premises infrastructure and gain access to scalable, modern platforms.

In practice, the results have often been more complicated. Undifferentiated migration, inconsistent workload assessment and unexpected consumption-based fees have contributed to rising costs. At the same time, some clinical workloads have proven difficult to move safely, efficiently or economically.

Healthcare organisations are now entering a more mature phase of cloud adoption. The question is no longer whether to use cloud, but how to operate the right mix of public cloud, private cloud and on-premises infrastructure for each workload.

Hybrid cloud is the practical answer for many healthcare environments, but it is not the simple answer. It introduces operational complexity that must be actively managed: workload placement decisions, data movement, identity and access controls, cyber monitoring, backup and recovery, interoperability, service management and cost governance all need to work consistently across multiple environments.

The first challenge is deciding where workloads should run. Not every application belongs in public cloud. Data-heavy and latency-sensitive workloads such as medical imaging may need to remain close to clinicians, diagnostic equipment and hospital networks to support performance and availability. Other workloads, such as analytics, AI development, collaboration platforms or non-clinical applications, may be better suited to hyperscale public cloud. A modern strategy requires disciplined workload classification rather than a default assumption that everything should move.



The second challenge is cost control. Cloud shifts expenditure from capital investment to consumption-based operating costs, which can improve flexibility but also create volatility. Without strong FinOps practices, health organisations can struggle to forecast, allocate and optimise cloud spend. Storage growth, data transfer, backup, testing environments and always-on resilience services can all create cost pressure if they are not governed from the start.

The third challenge is cyber security. Hybrid cloud expands the number of platforms, networks, identities and suppliers that need to be secured. In healthcare, where attackers target both sensitive data and operational disruption, security cannot be applied differently in each environment. Organisations need consistent controls, continuous monitoring, tested recovery and clear incident response processes across public cloud, private cloud and on-premises systems.

The fourth challenge is accountability.

Hybrid environments often involve multiple technology vendors, cloud providers, network partners, software vendors and internal teams. When performance degrades or an incident occurs, fragmented responsibility can slow resolution and increase clinical risk. For healthcare, the operating model must make accountability clear, with one view of service performance, risk, cost and clinical impact.

This is why hybrid cloud cannot be treated as a one-off migration or hosting choice. It is an ongoing operating discipline. Managing it well is complex, critical and difficult, particularly when clinical continuity, cyber resilience, cost control and patient trust are all at stake. Choosing the right partner is therefore not just a technology decision; it is a risk, resilience and service quality decision.



