CSL

Critical IoT Connectivity **Experts**

For CIOs, CCIOs, CSOs, clinical engineering, estates, and procurement leads

HEALTHCARE CONNECTIVITY ARCHITECTURE · PART 1 | SECONDARY CARE

Resilient Connectivity for Secondary Care

When signalling, cardiac telemetry, and clinical IT share one upstream path, a single outage becomes a site-wide incident.

Multiple domains

One shared dependency

A resilient design response

VERSION 4.1
DATE April 2026

1. Multiple Networks, One Hospital

EXECUTIVE SUMMARY

Hospitals do not run one network. They operate across multiple operational domains, each with different owners, different regulators, and different failure consequences, while often sharing a common upstream path.

A multi-domain model makes the shared dependency visible, so it can be documented, assessed, and governed.

An independent upstream path can also reduce cyber dependency risk: if ransomware compromises the Trust network, alarm signalling on a genuinely segregated path may remain available, provided routing, authentication, monitoring, and downstream dependencies are independently maintained.

Most NHS sites rely on fixed organisational connectivity (typically HSCN in England, SWAN in Scotland)[10]. That architecture is designed for clinical IT. But connected medical devices, estates systems, and third-party services each carry different ownership, different regulators, and different failure consequences.

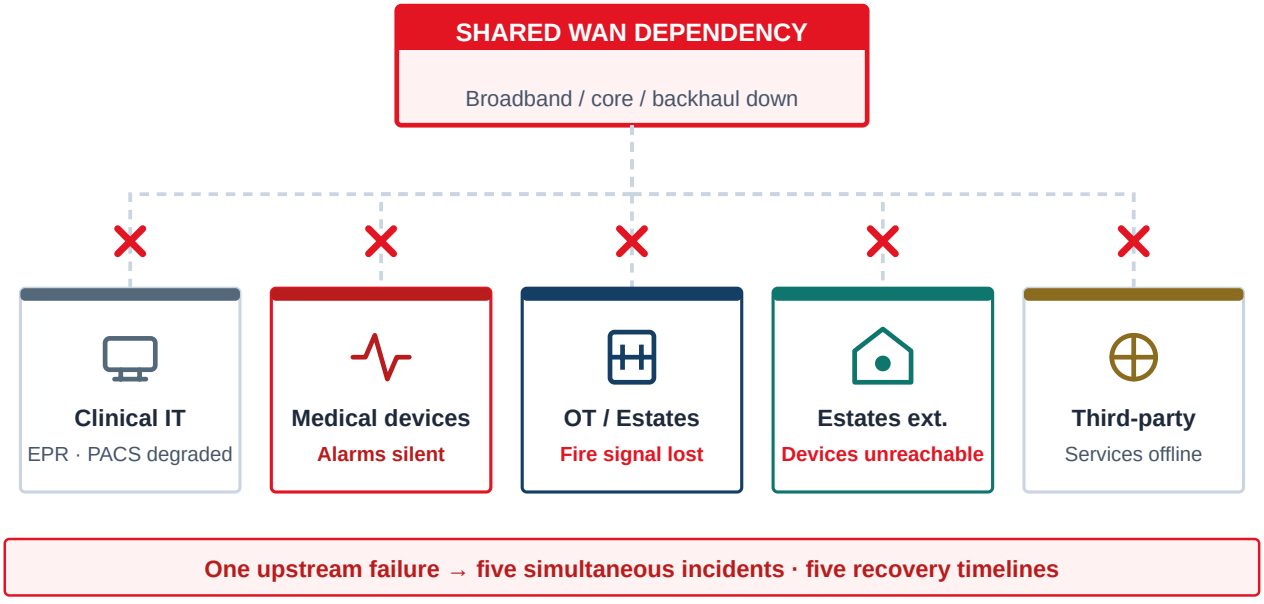
The critical design question is whether every other domain should inherit the Trust WAN by default. Where they do, the shared failure point should be documented and, if residual risk is unacceptable, separated[11].

What a shared outage looks like

Where multiple domains share an upstream path, a single failure can create concurrent incidents across otherwise separate services: loss of telemetry visibility, failed alarm transmission, interrupted estates signalling, and reduced access to clinical platforms. All from the same upstream event.

In practice: a cardiac alarm never reaches the central station; a fire panel sounds locally but the ARC signal fails silently; a lift alarm goes unanswered: all from one upstream failure.

Illustrative modelling using NHS Resolution CNST data (2024/25) indicates a material risk-weighted gap between shared-path and independent signalling for a cardiac monitoring fleet sharing a common upstream WAN[1]. Actual exposure depends on Trust-specific outage frequency, fleet size, and clinical pathway criticality. A worked example and assumptions are provided in Appendix B, p. 12.



One upstream failure → five simultaneous incidents · five recovery timelines

Why multiple domains, not one network?

The cascade diagram shows what happens when outer domains inherit a shared upstream path. The question is not whether lateral segmentation exists – most hospitals already have VLANs – but whether the *upstream* dependency is documented, separated, or explicitly accepted.

Different owners

Trust IT, clinical engineering, and estates are not one team.

Different regulators

Clinical safety, cyber assurance and life-safety signalling are governed through different assurance routes, standards, and operating responsibilities.

Different consequences

EPR downtime is not the same incident as a silent cardiac telemetry alarm, a failed fire panel signal, or a lost PACS connection in radiology.

Different recovery timelines

Restoring clinical IT after a WAN failure follows IT change control. Restoring fire panel signalling, lift alarms, or cardiac monitoring follows different procedures, different teams, and different urgency levels.

Board-level takeaway: document where the external failure point is shared, where it is separated, and where residual risk sits; before a single failure cascades across governance domains.

> ***"A silent alarm is not the same incident as IT downtime. The consequence profile is fundamentally different."***
>
> MULTIPLE NETWORKS, ONE HOSPITAL

NHS incident context: the pattern is documented

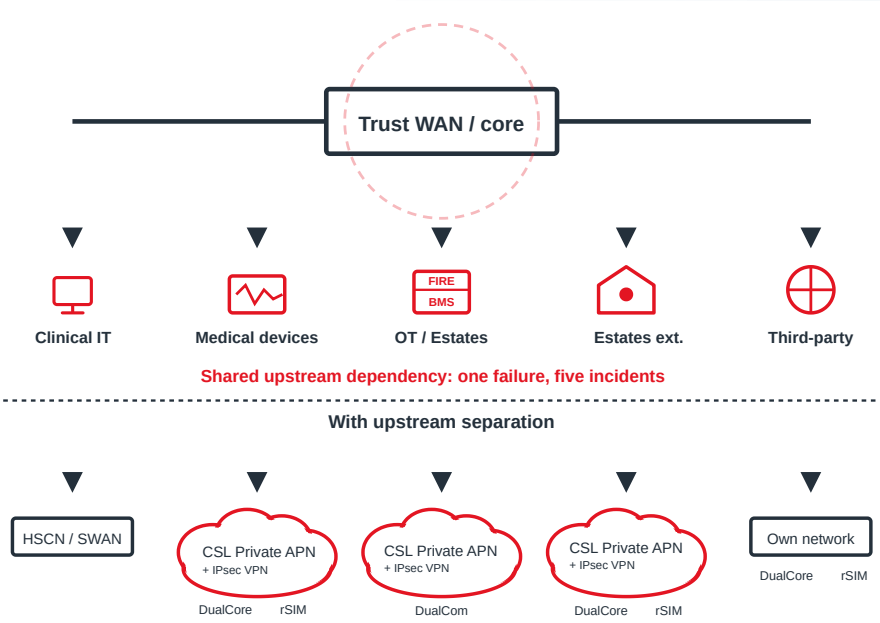
Recent NHS incidents confirm the pattern. In June 2024, the Synnovis ransomware attack reduced pathology capacity across south-east London, delaying over 11,000 appointments across multiple hospitals and clinics that shared a single supplier path[12]. In July 2024, NHS England reported that a global IT outage and a linked clinical system failure caused disruption in the majority of GP practices, with paper records and handwritten prescriptions used as contingency measures[13]. In July 2025, Gloucestershire Hospitals reported IT disruption from a routine server issue, not a cyber event[14]. Earlier, the 2022 ransomware attack on Advanced disabled NHS 111 and left some trusts without clinical records for months[15].

These incidents primarily affected clinical IT systems. The relevance here is structural: where alarm and life-safety systems share the same upstream path as clinical IT, the dependency pattern is similar even if it has not yet been separately documented. That parallel risk, silent loss of signalling on the same path, is harder to detect because it produces no visible error. A failed EPR produces a visible error on screen. A failed fire panel signal or cardiac alarm that never reaches the monitoring station produces no error message at all.

Separately, HSSIB's 2025 thematic review found that EPR system problems could contribute to missed, delayed, or incorrect patient care, and highlighted challenges with hardware and Wi-Fi availability in clinical environments[16]. A 2024 BBC FOI investigation reported 126 instances of serious harm linked to IT issues across 31 trusts[17]. The concern is not limited to cyber events; it extends to functional availability at the point of care.

SHARED DEPENDENCY RISK

One estate. Multiple domains. One avoidable failure point.



Clean separation is not about drawing more VLANs. It is about showing which pathways still fail together when a shared WAN or hosted core is lost.

DIFFERENT CONSEQUENCE

A silent alarm has a fundamentally different consequence from IT downtime.

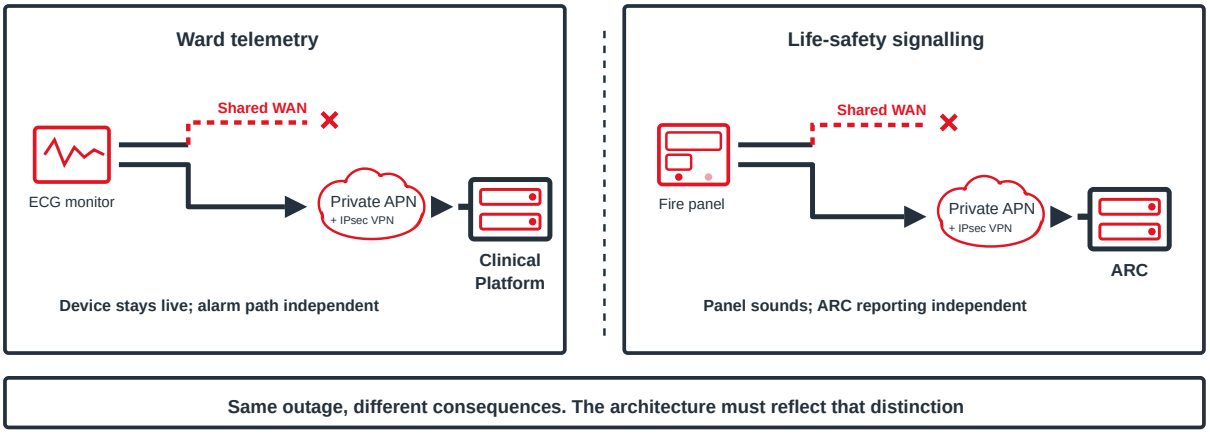


Figure 1: Ward telemetry vs life-safety signalling. Independent alarm paths can remain available when the shared WAN fails.

Why this matters for connectivity planning: A clinical IT outage triggers known workarounds. A silent alarm may not be detected until harm has occurred. Both stem from the same upstream failure, but the consequence profile, and the required response, are fundamentally different.

2a. Clinical IT & Connected Medical Devices

Clinical IT is the baseline. Medical devices add the upstream alarm dependency.

EPR / PAS & PACS

The electronic patient record and diagnostic imaging depend entirely on upstream WAN connectivity. A WAN outage means no EPR access and no remote radiology reporting. Offline access is typically limited, and sites often depend on paper-based contingency procedures rather than full digital continuity.

Cardiac monitors & vital signs

Continuous ECG and vital signs monitoring across CCU, ICU, and telemetry wards. The bedside unit continues locally during a WAN outage, but alarm transmission to the central monitoring station can be lost if the upstream path depends on the shared clinical WAN. That silent alarm gap during a cardiac event is a patient-safety risk.

Infusion pumps & syringe drivers

Smart pumps delivering precise drug doses across ICU, oncology, and surgical wards. Dose-error and occlusion alarms are safety-critical. If the alarm path depends on the clinical WAN, the safety net disappears during an outage.

Mobile & untethered devices

Ambulatory ECG holters, infusion pumps during transport, paramedic handover devices. These cannot connect to ward Wi-Fi and need managed cellular as their primary and sometimes sole data path.

EVIDENCE

The core risk: a medical device may continue to function locally during a WAN outage, while its upstream alarm path becomes unavailable. The monitoring platform or ARC receives nothing. Whether a given device can support an independent upstream path depends on OEM firmware and clinical safety approval, which vary by manufacturer.

Implementation example: DualCore rSIM

A drop-in SIM replacement for existing cellular medical devices. rSIM provides an independent upstream alarm and telemetry path from each device, so a WAN or broadband failure does not silence clinical alerts.

How it works: two physically separate operator cores with SIM-resident failover. Private APN + VPN encryption on both cores. No hardware replacement, and typically no firmware change where supported by the device[4].

For in-hospital devices: the device stays on the ward LAN; rSIM provides the independent upstream path. **For community/home devices:** rSIM is the primary connection, not a backup.

Implementation example: Outpost

Quad-radio hub for ward-level aggregation. Where multiple devices on a single ward need independent upstream connectivity, Outpost aggregates their traffic through a managed cellular path with PACE failover architecture.

"A cardiac monitor continues to display locally, but the alarm fails to reach the central monitoring station: creating an undetected patient-safety gap".

2b. Estates, Life Safety & Building Systems

Estates systems are governed separately from clinical IT, with distinct regulators and maintenance windows.

Fire panels

Hospital sites typically operate one or more master fire panels. The internal fire loop is hardwired; the upstream signalling path to the ARC is where connectivity matters. If fire signalling shares the clinical WAN, an IT outage means the ARC receives nothing.

Lift alarms

BS EN 81-28 covers trapped-passenger alarm communications. PSTN lines are being switched off; replacement paths that share the clinical WAN introduce dependency on infrastructure the estates team does not control.

BMS, CCTV & access control

Theatre air handling, pharmacy environmental monitoring, perimeter CCTV, and controlled-entry security. If BMS shares the clinical WAN, an IT change window can affect environmental control without warning.

Medical gas & water safety

Pipeline pressure monitoring (HTM 02-01) and Legionella temperature logging (HTM 04-01). Because these sit under estates governance and carry compliance consequences, a segregated estates path is often easier to assure than a shared clinical IT path.

EVIDENCE · SIGNALLING PATH ASSURANCE

The regulatory context: Where remote fire alarm transmission to an ARC is required, the signalling path should be assured against BS 5839-1 and BS EN 54-21 requirements. A shared Trust IT WAN may be difficult to justify if it cannot demonstrably meet those assurance requirements.

Implementation example: DualCom Pro

Dedicated dual-path ARC signalling from the master fire panel, independent of both clinical LAN and broadband. Supports BS 5839-1 / EN 54-21 signalling path assurance.

For lift alarms: CSL VoiceLink provides a managed cellular replacement for PSTN lift alarm signalling, subject to lift/alarm supplier design and local assurance.

Implementation example: Outpost

Quad-radio estates aggregation hub. BMS, CCTV, access control, nurse call, medical gas, and water safety monitoring connect through Outpost to a managed cellular path with Private APN + VPN.

What this means for Trust IT: Fewer cross-domain incident tickets. Clearer blast radius on maintenance windows. Each domain owns its upstream path independently.

"Independent signalling paths are not a nice-to-have. They are the audit trail that proves life-safety was not left sharing an IT maintenance window".

3. The Architecture Gap

In-hospital medical devices connect to the ward LAN or Wi-Fi, but their upstream alarm and telemetry data needs a WAN path to reach a platform or ARC. Where that path shares the clinical broadband, a broadband outage leaves alarm data without a delivery route. Yet most cellular offerings use a **single hosted core**[3]: multiple radio networks converging onto one MVNO core, which gives radio diversity but not core diversity.

For high-consequence clinical and operational pathways, genuine **core independence** (two physically separate operator cores with SIM-resident failover) is a strong resilience requirement and should be explicitly assessed.

Equally important: **private data paths must apply to both cores**, not just the primary. A solution that routes alarm data through a Private APN on one operator but falls back to public internet routing on failover does not meet the resilience standard for life-safety or clinical signalling. Both paths should carry Private APN + VPN encryption from device to platform or ARC.

CYBER RISK

Security & cyber resilience

An independent upstream path mitigates a specific cyber vulnerability: if ransomware compromises the Trust WAN, every service sharing that path is affected, including alarm signalling. A separate Private APN + VPN path means traffic never touches the public internet, IPsec encryption applies on both cores, and no infrastructure is shared with the Trust WAN. The question is not whether cellular is as secure as HSCN; it is whether the same upstream dependency should carry both clinical IT and higher-consequence life-safety or alarm-signalling pathways.

NCSC CAF B5 · DSPT NETWORK RESILIENCE

Why does the upstream path matter?

When a medical device sends alarms over hospital Wi-Fi, that traffic shares the clinical WAN and broadband. When broadband fails, the alarm path fails with it, even if the device itself is still running.

In-building signalling resilience

Thick walls, basements, MRI-shielded rooms, and lift shafts create Wi-Fi dead spots. A cellular upstream path is independent of indoor Wi-Fi infrastructure, but dense construction can also attenuate cellular signal. Pre-deployment site surveys and external antenna options address coverage gaps.

Rural sites and GP broadband backup

Satellite sites and secondary buildings often have unreliable broadband. A managed cellular router provides failover: EPR, prescribing, and records stay online via Private APN + VPN.

Broadband-dependent devices

Some connected devices rely on domestic or site broadband with variable quality, no formal SLA, and limited Trust visibility over uptime. Where that broadband is the only upstream path, device data and alarms inherit its reliability. A managed cellular SIM gives each device its own independent path with defined service levels.

"Up" is not the same as "clinically usable"

A WAN that passes a ping test may still be degraded: packet loss, latency spikes, or congestion can make it unusable for time-sensitive alarm signalling. The clinical question is not "is the path up?" but "would a cardiac alarm reach the monitoring station within the required window?" An independent upstream path materially reduces this ambiguity by separating alarm and telemetry delivery from the Trust WAN.

BREAK-GLASS

Emergency break-glass backup

When the Trust WAN fails completely, a bonded quad-modem cellular uplink can provide emergency backup connectivity for essential clinical services (EPR access, prescribing, and discharge workflows) via Private APN + VPN, independent of the failed broadband or HSCN path.

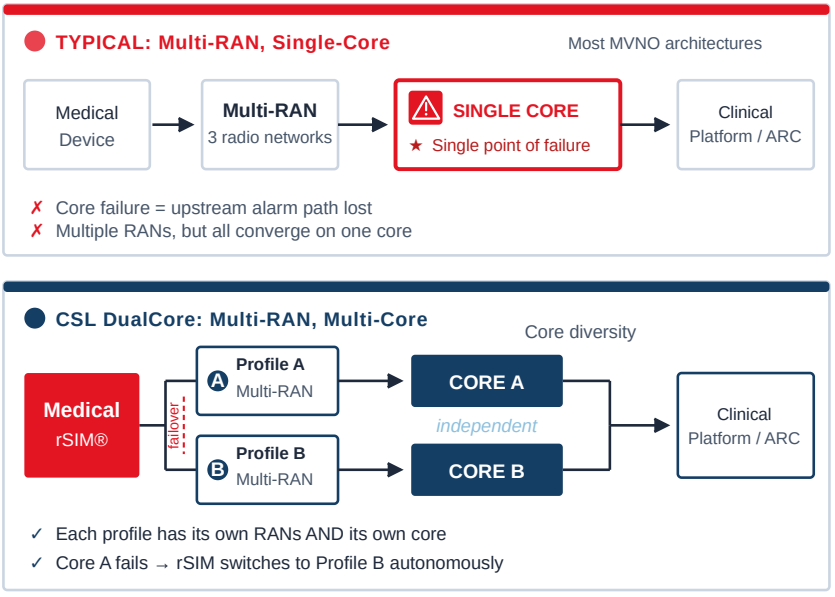


Figure 2: Single-core multi-RAN vs DualCore multi-core. True path diversity requires independent operator cores.

4. Compliance & the Regulatory Landscape

The architecture gap, a shared external path without core diversity, is not just a technical risk; it is a governance and regulatory exposure. No regulation mandates a specific network topology, but four frameworks require documented risk management, data security, and demonstrable availability. Upstream separation helps evidence each.

Security & cyber resilience

A shared external path is itself a cyber vulnerability. If a ransomware incident disables the clinical network, alarm signalling sharing that path can be silently disabled with it. Where alarm signalling uses a logically and operationally segregated path such as CSL's Private APN infrastructure, it may continue to function during a Trust-network cyber incident: Private APN traffic never touches the public internet; IPsec VPN encrypts data on both cores; no shared infrastructure or routing with the Trust WAN. This supports NCSC CAF Objective B5 and helps evidence DSPT outcomes for network resilience.

MHRA / UK MDR

For connected medical devices, the manufacturer's ISO 14971 risk management file should consider connectivity loss where it could affect safety or intended performance. A resilient, independently managed upstream path can support a documented risk-control entry for that hazard. Post-market surveillance obligations (effective 16 Jun 2025, per UK MDR 2002 as amended) also benefit from resilient connectivity[1].

DCB0129 / DCB0160: Clinical Safety

Both OEM manufacturers (DCB0129) and deploying organisations (DCB0160) must maintain a Clinical Safety Case and hazard log. Connectivity is a foreseeable hazard. An independent upstream path can support evidence for that hazard entry, subject to local clinical safety assessment[2].

GOVERNANCE

NHS DSPT (CAF-aligned, 2025–26)

DSPT v8 (2025–26) aligns to CAF v3.4. *(Note: NCSC has since published CAF 4.0; DSPT currently references v3.4; see note 5.)* **CAF B5** (Resilient Networks and Systems) states that *"systems are appropriately segregated and resource limitations are mitigated"* and that organisations should identify and address single points of failure in their network architecture. A multi-domain model supports CAF B5 by making segregation and single points of failure explicit[5].

GOVERNANCE

CQC Regulation 12

Safe Care & Treatment expects infrastructure that supports safe care delivery. Where a single point of failure exists on medical device connectivity, Trusts should document and assess the risk[6].

GOVERNANCE

NHS Procurement: DTAC

DTAC Form v2.0 takes effect from 6 April 2026 when requested by buyers[7], and is scoped to software-based digital health technologies. Where the product is DTAC-scoped, this connectivity architecture may support parts of the evidence set, but it does not itself satisfy DTAC and sits *alongside* wider procurement, clinical safety, and interoperability assessment.

GOVERNANCE

Clinical Safety Artefacts

Expect to produce: **CSO appointment** · **Hazard log** (connectivity as foreseeable hazard) · **Clinical Safety Case Report** · **Deployment Risk Assessment**. Connectivity separation is not a substitute for clinical safety case work, cyber assurance, or local governance.

> ***"No regulation mandates a specific network topology. But four key frameworks require documented risk management, data security, and demonstrable availability".***

5. Implementation Form Factors

Three design rules apply to every deployment, regardless of form factor or device category:

Rule 1
Independent upstream path: alarm and telemetry traffic does not share the clinical WAN.

Rule 2
Private routing on both cores: Private APN + VPN encryption applies on primary and failover, not just one.

Rule 3
Managed failover: SIM- or device-resident switching between physically separate operator cores, with staggered reversion at scale.

The choice of deployment model depends on device type, site topology, and local governance. The following examples show how these design rules can be implemented across different operational contexts, including segregated and secure broadband and satellite connectivity

PER-DEVICE SEPARATION

Deployment context: upstream signalling for hospital telemetry and infusion alarms; primary connectivity for CGM, CPAP, hospital-at-home kits, and community RPM devices.

A drop-in SIM for existing cellular medical devices. For in-hospital devices, rSIM provides an independent upstream alarm and telemetry path; the device can remain on the ward LAN while its outbound signalling takes an independent path, subject to OEM approval and local integration architecture. For community and home devices, rSIM is the primary resilient connection.

rSIM

rSIM®
Device-level resilience

PER-CIRCUIT SIGNALLING

Deployment context: hospital fire panels, medical gas manifold alarms, access-linked alarms, security signalling, and any panel that must report reliably even when the main site network is degraded.

Dedicated signalling hardware for fire panels, medical gas manifold alarms, and security systems. It keeps safety-critical alarm paths away from shared hospital broadband, delivering signals to third-party ARCs via private cellular connectivity.

DC

DualCom Pro
Life-safety and ARC signalling

SITE-LEVEL FAILOVER

Deployment context: satellite sites without fixed broadband, secondary estates compounds, and temporary clinical facilities.

A managed router for practices, clinics, community bases, and vehicles. It provides secure broadband resilience or a primary cellular path for sites without reliable fixed connectivity, using Private APN and managed VPN.

RTR

CSL IoT Router
Site failover and secure hotspot

MULTI-SERVICE AGGREGATION

Deployment context: acute sites, satellite hospitals, or estates compounds where several segregated services benefit from a single managed edge with a private operational handoff.

A multi-radio, multi-service edge appliance for sites with several outer networks. It aggregates upstream medical device signalling, nurse call, estates, and alarm traffic onto an independent path, keeping those flows off the clinical WAN. In a total site outage, Outpost can also provide emergency break-glass connectivity via its bonded cellular uplink.

OUT

CSL Outpost
Hospital edge aggregation

SITE SURVEY

Deployment context: pre-installation site surveys for acute hospitals and satellite sites, and any site where in-building cellular coverage needs validation before device deployment.

A handheld multi-network signal survey tool that identifies the strongest available mobile network at each installation point. Surveys multiple operators and frequencies simultaneously, producing exportable reports for documentation and sign-off. Removes guesswork from device placement in lead-lined rooms, basement plant areas, and shielded zones.

CSL Signal Analyser 2
Pre-deployment site survey

PSTN REPLACEMENT

Deployment context: lift alarm panels requiring PSTN replacement under BS EN 81-28, and any trapped-passenger or building alarm that previously relied on analogue phone lines.

A managed cellular voice and data gateway replacing PSTN connections for lift alarms and other building safety systems. VoiceLink maintains trapped-passenger alarm communications via Private APN, independent of the clinical WAN and broadband.

VL

CSL VoiceLink
PSTN replacement for lift & building alarms

6. Next Steps

Clinical IT belongs on the organisational WAN. But outer domains often inherit that same path by default. The question is where a common failure point creates unacceptable risk, and how to address it pragmatically.

How a Trust would apply this in practice

1. Identify one high-risk pathway or asset class (e.g. cardiac telemetry, infusion alarms).

2. Map current WAN and upstream dependency for that pathway.

> **Support for Steps 1–2:** a managed connectivity partner can provide a dependency mapping workshop (typically 1–2 weeks, covering device estate audit, shared-path identification, and upstream risk register).

3. Confirm governance owners across CIO, CCIO, CSO, clinical engineering, estates, and cyber.

4. Define whether separation is required, desirable, or unnecessary, based on criticality and recoverability.

5. Pilot one pathway: test failover and downtime procedures in a live environment.

6. Scale only after clinical safety and operational sign-off.

"Connectivity segregation does not replace governance. It makes dependency visible so governance can act."

Pre-deployment checklist

☐ **Core independence confirmed:** provider demonstrates physically separate operator cores with independent subscriber management, not shared MVNO infrastructure.

☐ **Private APN on both cores:** end-to-end VPN encryption; no public internet breakout on either path.

☐ **Clinical safety hazard log updated:** connectivity as foreseeable hazard documented per DCB0129/DCB0160.

☐ **Site survey completed:** in-building cellular coverage validated at each installation point before device deployment.

☐ **Failover SLA agreed:** documented failover time, monitoring scope, and escalation path in managed service contract.

☐ **Reversion plan documented:** staggered migration back to primary after outage; signalling surge management at scale.

☐ **OEM integration confirmed:** device manufacturer supports rSIM or independent upstream routing under current firmware.

☐ **Cyber separation validated:** independent path does not share infrastructure, routing, or credentials with the Trust WAN; traffic never traverses public internet.

☐ **Local risk acceptance recorded:** where shared dependency is retained, documented as accepted risk with named owner.

Where separation is most likely to matter first

High-acuity monitoring and alarm workflows (cardiac telemetry, vital signs) · infusion and drug delivery pathways (PCA, syringe drivers) · fire, life-safety and critical estates controls · PACS/radiology where image transfer depends on shared bandwidth · pathology partner systems with third-party connectivity · mixed operational environments. NHS England's Networks & Connectivity Programme (Frontline Productivity) is actively supporting wireless and IoT connectivity across NHS sites and into the community[10].

Start here: Life-safety signalling (fire panels, lift alarms) and high-acuity telemetry (cardiac monitors, infusion pumps) carry the highest consequence of shared-path failure and are typically the fastest to separate, often without disrupting the existing ward LAN. Begin with one pathway, validate the architecture, then extend.

Governance & assurance responsibilities

Connectivity segregation does not replace local governance. Trusts should ensure clinical safety ownership remains with the responsible manufacturer (DCB0129) and deployer (DCB0160); local risk acceptance, change control, and cyber review are completed before deployment; and supplier due diligence covers connectivity, failover SLA, and data handling.

6. Next Steps (continued)

Illustrative NHS deployment examples

Cardiac telemetry fleet: A Trust with 200+ cardiac monitors across CCU, ICU, and telemetry wards identifies that upstream alarm traffic shares the clinical broadband. An rSIM swap for each device's cellular module provides an independent alarm path without replacing the ward LAN and, where supported by the OEM and current device configuration, without changing device firmware.

Fire panel signalling (PSTN replacement): With PSTN switch-off approaching, a Trust's 12 networked fire panels need a replacement ARC signalling path. DualCom provides dual-path cellular signalling from the master panel, independent of the clinical WAN, supporting BS 5839-1 / EN 54-21 signalling path assurance.

Satellite site broadband resilience: A community hospital with a single broadband circuit and no HSCN connection loses EPR access during outages. A CSL IoT Router provides managed cellular failover via Private APN + VPN, keeping prescribing and discharge workflows online.

Procurement routes

Independent upstream connectivity does not need to be procured through the clinical WAN route. Existing NHS frameworks already cover IoT, smart technologies, and mobile data as separate lots. This means estates and medical device connectivity can be procured independently of clinical WAN contracts, consistent with the multi-domain model. Framework references are in the source notes[9]; confirm current status with your procurement team before use.

Private 5G and neutral-host integration

Where a Trust has deployed or is deploying a private 5G or neutral-host network on campus, a dual-profile SIM architecture can accommodate it. One profile could connect to the on-campus private network, with automatic failover to a macro cellular network on the second profile. This requires collaboration between the Trust (or neutral-host operator) and the connectivity provider, but the underlying architecture is designed to support it. As NHS Trusts explore private 5G for IoMT and in-building coverage, this creates a path where on-campus connectivity and independent upstream resilience coexist within the same SIM.

Companion paper: The same connectivity architecture principles extend beyond the acute site to GP surgeries, community clinics, Hospital at Home, telecare, and mobile clinical teams. For the equivalent analysis applied to primary care and community settings, see *Resilient Connectivity for Primary Care & Community*.

Next steps

Web: csl-group.com
Email: sales@csl-group.com
Phone: +44 (0) 1895 474 474

For detailed cost-of-downtime modelling and zone-level exposure analysis, CSL can support an initial scoping conversation for Trust-specific planning.

Where full separation may not be necessary

Not every connected asset requires full path independence. Bedside entertainment, managed print, staff Wi-Fi, non-critical BMS sensors, and supplier-managed catering POS may justify shared dependency where the clinical and operational risk is understood, documented, and accepted. The goal is not universal separation. It is explicit risk acceptance where shared dependency remains.

"The goal is not universal separation. It is explicit risk acceptance where shared dependency remains".

Bridge to Part 2: Community & Home Connectivity

The same architecture principle that protects hospital domains, independent upstream paths segregated from the shared WAN, applies beyond the hospital wall. But the operating context is fundamentally different: there is no managed WAN to segregate from, no on-site IT team, and no single commissioner.

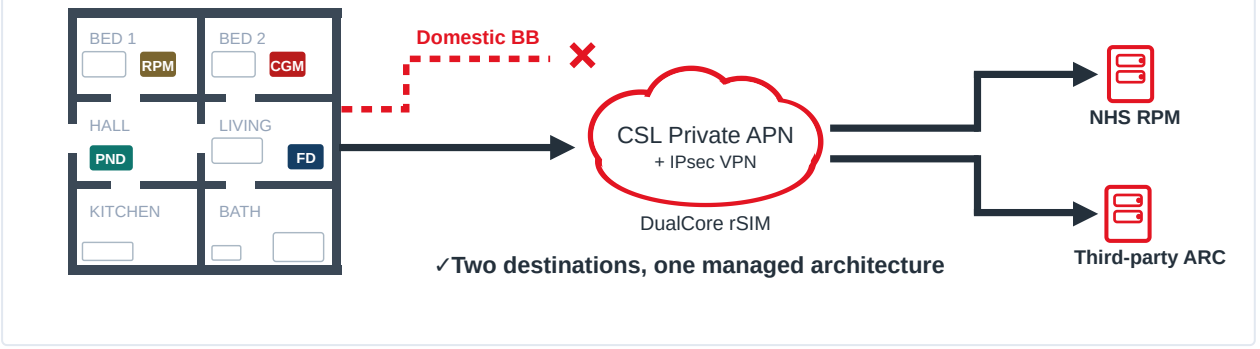


Fig 3 One managed path can serve both RPM and third-party ARC

Remote patient monitoring and alarm escalation need not depend on domestic broadband when one managed cellular architecture serves both destinations.

RPM Remote patient monitoring · CGM Continuous glucose monitor · PND Pendant alarm (telecare) · FD Fall detector

The full primary care and community case is in Part 2

The companion paper, *Resilient Connectivity for Primary Care & Community* (Part 2 in this series), addresses the specific challenges of GP surgeries, remote clinics, Hospital at Home, RPM, council telecare, and the PSTN switch-off. It also includes a standalone *Minimum Architecture Standard* that applies to any primary care deployment regardless of site type or commissioner.

"Community and home devices have no ward LAN at all. Managed cellular is their primary connection, not a backup".

Appendix B: Supporting Business Case

This appendix provides an illustrative scenario model for planning and decision-support only. It is not presented as direct empirical proof of outage cost. Downtime cost inputs use NHS England National Cost Collection 2024/25 and NHS Resolution CNST 2024/25 as reference inputs[11].

For a 200-device cardiac monitoring fleet sharing a common upstream WAN, this illustrative model indicates a risk-weighted exposure gap of approximately £0.55m per year under the stated assumptions. Actual exposure will depend on Trust-specific fleet size, outage frequency, recovery time, pathway criticality, and local cost assumptions. Independent validation is recommended before business-case submission.

Worked calculation: simplified risk-exposure model

```
Annual risk exposure = Fleet × Outages/yr × Recovery hrs × Blended cost/device-hr
```

Input	Value	Source
Fleet size	200 monitors	Illustrative (CCU, ICU, telemetry wards)
Upstream outage events	3/year	NHS England incident reporting
Mean recovery time	4 hours	NHS England incident reporting
Blended cost per device-hour	£242	Derived from NHS Resolution CNST cardiology avg. total settlement value (£113k/claim, 2024/25; damages plus claimant and NHS legal costs, Additional Annual Statistics Sheet 4)[11] and National Cost Collection 2024/25

Single-LAN exposure: 200 × 3 × 4 × £242 = **£580.8k/year**

With independent upstream path: if Dual-Core separation reduces upstream outage exposure by 90–99%, residual risk falls to **£58k–£6k/year**. At a mid-range assumption of 95%, residual ≈ £29k/year. Trusts should set this parameter based on local outage data and upstream path architecture.

This is a simplified linear approximation. The blended cost-per-device-hour is derived from the general CNST cardiology claims pool; it assumes connectivity-related incidents would produce a comparable claims profile, which Trusts should validate against their own pathway and acuity mix. NHS Resolution 2024/25 data shows £3.08bn in total clinical negligence payments across all schemes (CNST: £2.82bn), with 197 CNST cardiology claims settled in 2024/25 at an average £113k total settlement value per claim (damages plus claimant and NHS legal costs; NHS Resolution Additional Annual Statistics, Sheets 2 and 4, 2024/25)[11]. Actual exposure depends on Trust-specific fleet size, outage frequency, and cost parameters.

How an independent upstream path works

A resilient SIM authenticates directly to a Private APN on the macro cellular network. An IPsec VPN tunnel encrypts all traffic from device to platform or third-party ARC. If the primary operator core becomes unavailable, the SIM switches automatically to a physically separate secondary core with its own Private APN and VPN tunnel. No shared routing, authentication, or infrastructure exists between the two paths or with the Trust network. The result: an alarm and telemetry path that remains operational even when the hospital's own broadband, WAN, or hosted core is down. CSL's DualCore rSIM implements this architecture with SIM-resident failover between two independent operator cores.

Deployment pathways

rSIM swap
Drop-in SIM replacement for existing certified devices. No hardware replacement, and typically no firmware change where supported by the device. Fastest path to Dual-Core resilience.

CSL IoT Router
Managed cellular router with built-in DualCore resilience. Replaces or supplements site router for multi-device categories.

CSL Outpost
Quad-radio hub for large sites aggregating multiple device categories. PACE architecture: Primary + Alternate + Contingency + Emergency.

Managed reversion at scale

When a network recovers, every displaced device reconnects simultaneously, risking a signalling surge. Dual-Core deployments at scale should include staggered reversion: managed migration back to primary over a controlled window[1].

"If Profile A's operator core becomes unavailable, the rSIM switches automatically to Profile B on a physically separate core with its own Private APN and VPN tunnel".

Appendix C: OT & Life-Safety Layer Diagram

Fire detection, lift alarms, nurse call, medical gas monitoring, water safety, CCTV, access control, EV charging, and BMS connectivity. A large hospital typically uses multiple CSL products across three distinct connectivity paths: DualCom for fire panel ARC signalling, VoiceLink for lift alarm signalling, and Outpost for estates aggregation, all independent of the clinical LAN and WAN. Device placement is illustrative.

Life safety + estates controls | **Private APN + VPN** | **Illustrative placement**

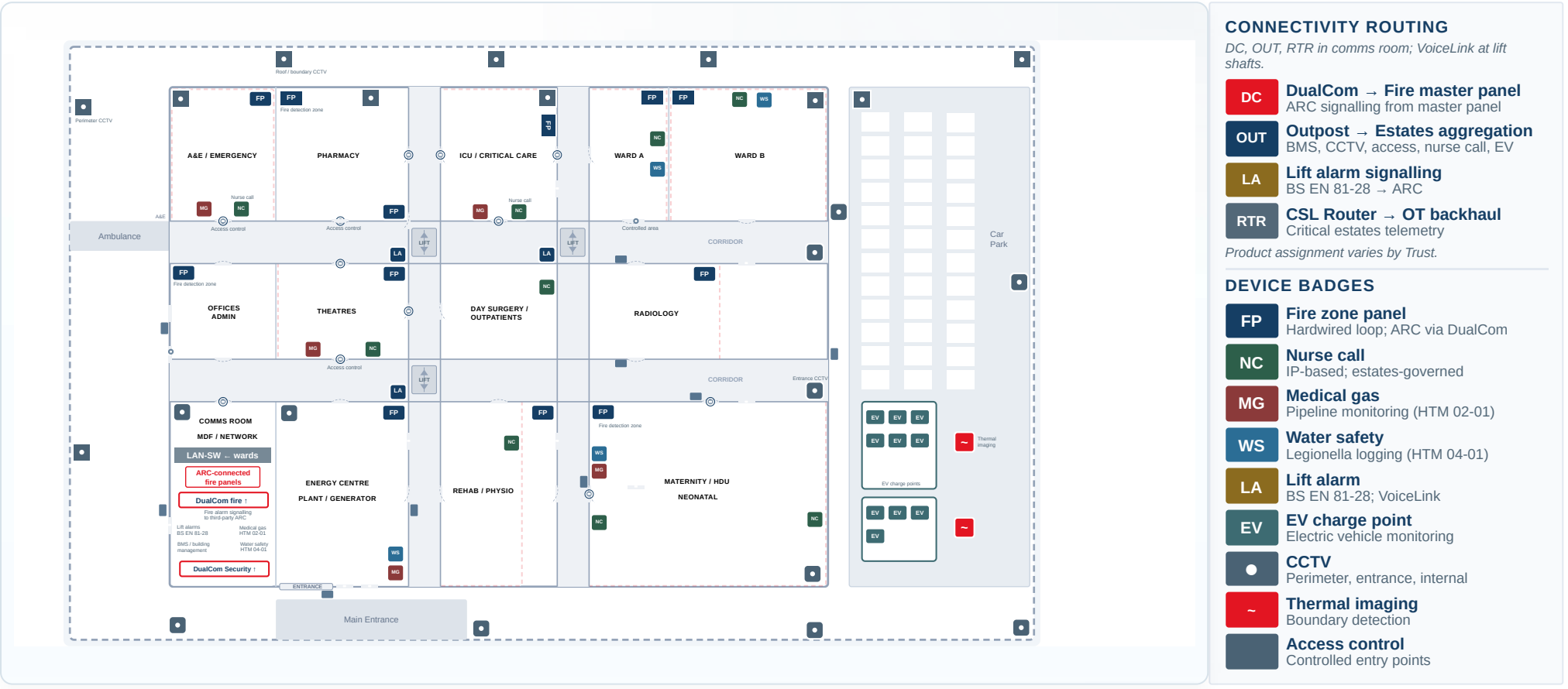


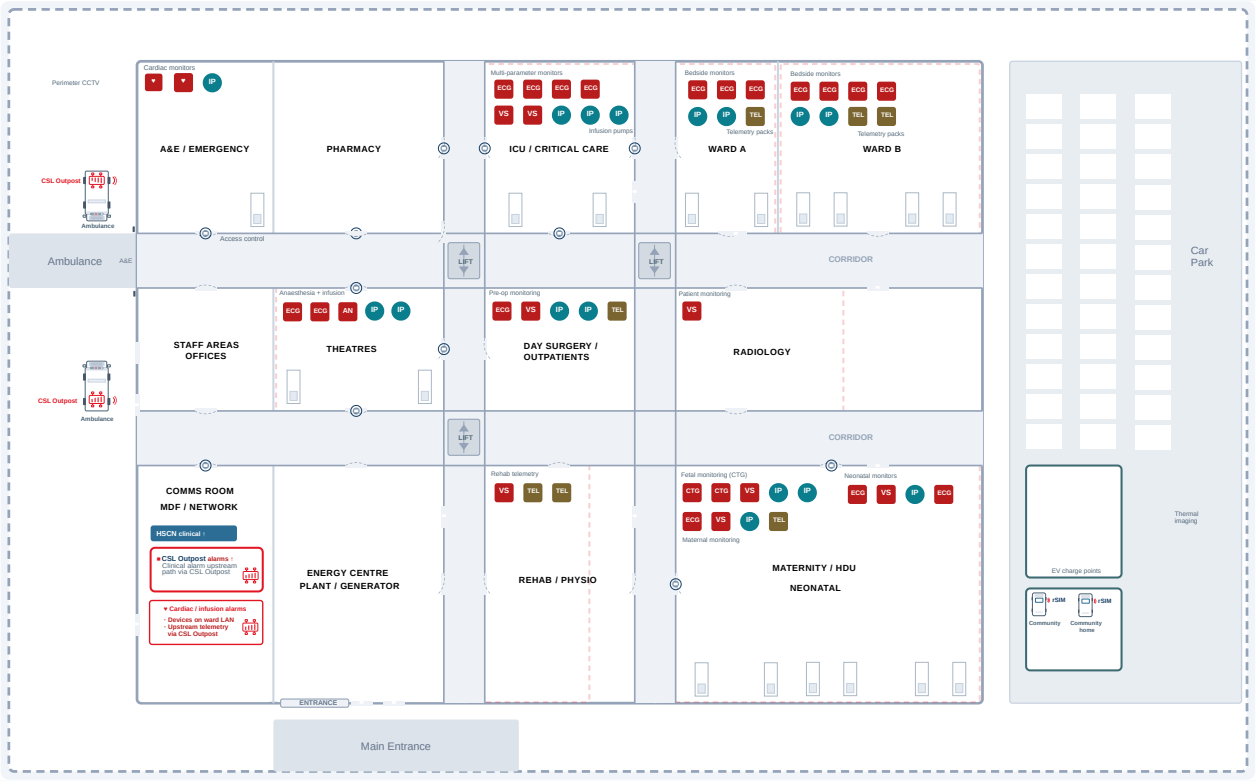
Figure 4: OT & life-safety connectivity layer. Fire zone panels (FP) connect via the networked fire loop to a master panel; a DualCom provides dual-path ARC signalling from that master panel. Estates systems (BMS, CCTV, access control, nurse call, medical gas, water safety, EV chargers) aggregate through one or more CSL Outpost units or CSL Routers. Lift alarms (BS EN 81-28) connect via CSL VoiceLink as a managed cellular replacement for PSTN signalling. All CSL paths use Private APN + VPN, fully segregated from the clinical LAN and WAN. Actual product assignment varies by Trust estate.

Note: FP badges on this diagram represent fire zone panels on the internal networked fire loop, not individual signalling endpoints. A single DualCom typically connects at the master fire panel to provide dual-path ARC signalling for the entire fire system. Broader estates devices connect via one or more CSL Outpost units or CSL Routers, depending on failover requirements and Trust-specific architecture.

Appendix D: Medical Technology Layer Diagram

Cardiac monitors, vital signs, infusion pumps, and RPM devices. In-hospital devices typically connect via ward LAN with independent upstream alarm and telemetry paths via CSL Outpost, segregated from the clinical WAN. Community and home-monitoring devices connect directly via DualCore rSIM as the primary path. Device placement is illustrative.

Telemetry + alarms | **Independent upstream path** | **Community / home via rSIM**



CONNECTIVITY ROUTING

Outpost in comms room; rSIM per device.

- **OUT** — **Outpost → Upstream alarms**
  ECG, VS, IP on ward LAN → ARC
- **rSIM** — **DualCore rSIM → Primary path**
  Community RPM, CGM, CPAP
- **IP** — **Infusion → ward LAN + rSIM**
  Alarm upstream via Outpost
- **TEL** — **Telemetry → Continuous**
  Real-time cardiac data to clinical platform

ward LAN for local; Outpost/rSIM upstream.

DEVICE BADGES

- **ECG** — **Cardiac monitor**
  CCU, ICU, telemetry wards
- **VS** — **Vital signs**
  SpO_2, BP, temperature
- **IP** — **Infusion pump**
  Dose-error and occlusion alarms
- **AN** — **Anaesthesia workstation**
  Theatre delivery and monitoring
- **CTG** — **Cardiotocograph**
  Fetal heart rate; maternity/HDU
- **TEL** — **Telemetry pack**
  Ambulatory cardiac monitoring

Figure 5: Medical technology connectivity layer. Cardiac monitors, vital signs, infusion pumps, and RPM devices. In-hospital devices typically retain the ward LAN for local connectivity, while CSL Outpost provides an independent upstream alarm and telemetry path where supported by device integration and local governance. All CSL paths use Private APN + VPN.

Note: CSL does not replace the ward LAN for in-hospital devices. Where a medical device connects locally via the ward network, CSL Outpost provides an independent upstream path for alarm signalling and telemetry, so that a WAN or broadband failure does not silence clinical alerts. For community and home devices, rSIM is the primary connectivity path with no dependency on shared broadband.

About CSL Group

CSL Group is a UK and EU telecommunications company specialising in resilient connectivity for critical IoT. With a Private APN + VPN infrastructure supporting over 3.5 million active connections[8], CSL provides the outer connectivity layer, independent of the clinical WAN (HSCN / SWAN), for medical devices, estates systems, and site resilience.

Evaluation criteria for upstream connectivity providers

Core architecture: Ask whether resilience is delivered through physically separate operator cores with independent subscriber management, or through radio profiles routed via a shared MVNO infrastructure. The distinction determines whether a single core failure affects both paths.

Deployment model: Understand whether resilience requires firmware changes to each device (with associated clinical safety implications) or operates at the SIM layer independently of device software. This affects deployment timescale, OEM dependency, and change-control burden.

Security and compliance posture: Verify that both connectivity paths use Private APN with end-to-end VPN encryption and no public internet breakout. This supports DSPT/CAF B5 evidence requirements and may contribute to B3/B4 outcomes depending on implementation.

Operational heritage: Assess whether the provider has a track record in life-safety and critical signalling, not just commercial IoT. Private VPN connectivity to alarm receiving infrastructure demonstrates operational maturity in environments where connectivity failure has direct safety consequences[8].

Managed service scope: Confirm whether connectivity, failover, monitoring, and SIM lifecycle are consolidated under a single provider and contract, or split across multiple parties with separate accountability.

In-building validation: Dense hospital construction attenuates cellular signal. Confirm the provider's approach to pre-deployment site surveys, multi-operator coverage options, and antenna solutions for challenging environments.

Scope & limitations

This paper presents an illustrative architecture model, not a universal deployment prescription. It does not substitute for clinical safety case work, cyber assurance, or local governance. The multi-domain model is a decision framework for documenting where operational domains share a common external path. Applicability depends on device type, OEM integration, local architecture, and governance route. Trust-specific validation is required before procurement.

Key message: a shared upstream path is a documentable, assessable risk, not an inevitability. Where alarm, telemetry, and life-safety signalling share a common WAN path with clinical IT, the architecture should make that dependency explicit. Where the risk is unacceptable, separation is a design choice that can be implemented without replacing existing ward infrastructure.

Further reading from CSL Group

IoMT Regulatory Pathways & Evidence for NHS Adoption: UKCA/CE conformity assessment, NICE Evidence Standards Framework, DTAC, and virtual ward integration checklists.
csl-group.com/white-papers/iomt-regulatory-pathways-evidence-nhs-adoption

The Future of Healthcare: How IoMT and AI Are Transforming Care Delivery: Resilient connectivity, cybersecurity, interoperability, and compliance for connected health at scale.
csl-group.com/white-papers/telecare-healthcare-iomt-ai-transforming-healthcare

The Future of Healthcare, Telecare and the Internet of Medical Things: Policy, demographic, and clinical context driving adoption of remote care technologies.
csl-group.com/white-papers/future-of-healthcare-telecare-internet-of-medical-things-iomt-part1

Healthcare & Telecare Solutions: CSL's connectivity portfolio for NHS, telecare, and Hospital at Home deployments.
csl-group.com/sectors/healthcare-telecare

Sources & notes

OFFICIAL & PUBLIC SOURCES

[2] NHS England, DCB0129 & DCB0160. Refer to NHS England for current editions.
digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards

[5] DSPT v8 (2025–26) aligns to CAF v3.4. NCSC's own published changelog lists versions 3.0, 3.1, 3.2, and 4.0; the v3.4 numbering appears to be the DSPT's sector-specific adaptation reference. NCSC has since published CAF 4.0 (Aug 2025). CAF B5 calls for appropriate segregation and single-point-of-failure identification. B3 calls for access-controlled pathways. Submission deadline 30 Jun 2026. Verify current deadline with NHS England.
dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides
ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b5-resilient-networks-and-systems

[6] CQC Regulation 12 (Safe care and treatment).
cqc.org.uk/guidance-regulation/providers/regulations-service-providers-and-managers/health-social-care-act/regulation-12

[7] DTAC: transition effective 6 April 2026.
transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac

[9] Procurement routes (status as at April 2026; verify current availability with your procurement team before use): HSCN DPS RM3825; GCA RM6261 Mobile. RM6116 Network Services 3 (now under GCA, formerly CCS) was extended to 17 Jul 2027. CCS became the Government Commercial Agency (GCA) on 1 Apr 2026. Framework detail changes frequently; verify current availability before use.
crowncommercial.gov.uk/agreements/RM3825
crowncommercial.gov.uk/agreements/RM6261
crowncommercial.gov.uk/agreements/RM6116
gca.gov.uk/news/introducing-government-commercial-agency

[10] NHS England Internet First.
digital.nhs.uk/services/internet-first

[11] NHS Resolution Annual Report 2024/25: total clinical negligence payments £3.08 bn across all schemes (Supplementary Annual Statistics, Sheet 1); CNST £2.82 bn. Cardiology: 197 CNST claims at £113 k average total settlement value per claim (damages plus legal costs; Additional Annual Statistics, Sheets 2 and 4). Figures are illustrative; validate against Trust-specific fleet data.
resolution.nhs.uk/wp-content/uploads/2025/07/E03358428-NHS-Resolution-ARA-24-25-Web-accessible.pdf

National Cost Collection 2024/25 provides Trust-level reference costs.
england.nhs.uk/publication/2024-25-national-cost-collection-data-publication

[12] NHS England, Synnovis ransomware incident (Jun 2024). Services not fully restored until Dec 2024.
england.nhs.uk/synnovis-cyber-incident

[13] NHS England statement on GP clinical system disruption during global IT outage (19 Jul 2024).
england.nhs.uk/2024/07/response-to-global-it-outage

[14] Gloucestershire Hospitals NHS Foundation Trust, IT disruption from 22 July (23 Jul 2025).
gloshospitals.nhs.uk/about-us/news-media/press-releases-statements/it-disruption-22-july

[15] ICO enforcement decision on Advanced Computer Software Group (Mar 2025).
ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited

[16] HSSIB, Electronic patient record systems: thematic review (2025).
hssib.org.uk/patient-safety-investigations/electronic-patient-record-epr-systems-thematic-review

[17] BBC / Digital Health FOI investigation (2024). Press-reported FOI output, not an official NHS statistical series. Figures cited are as reported by the original investigation; verify against Trust-level reporting before use in formal submissions.
digitalhealth.net/2024/05/bbc-investigation-links-nhs-it-failures-to-patient-harm

MHRA post-market surveillance requirements for medical devices in Great Britain. PMS requirements in force from 16 Jun 2025.
gov.uk/government/publications/medical-devices-post-market-surveillance-requirements

SECTOR & INDUSTRY COMMENTARY

[3] MVNO core architectures vary; verify core independence with provider topology documentation.

[4] rSIM SIM-swap classification: confirm with device manufacturer under applicable MHRA/MDR guidance.
gov.uk/guidance/medical-devices-get-regulatory-advice-from-the-mhra

[8a] Lift alarm signalling: BS EN 81-28:2022.
knowledge.bsigroup.com/products/safety-rules-for-the-construction-and-installation-of-lifts-lifts-for-the-transport-of-persons-and-goods-remote-alarm-on-passenger-and-goods-passenger-lifts-1

[8b] Medical gas pipeline systems: HTM 02-01.
england.nhs.uk/wp-content/uploads/2021/05/HTM_02-01_Part_A.pdf

[8c] Water safety: HTM 04-01.
england.nhs.uk/wp-content/uploads/2021/05/DH_HTM_0401_PART_A_acc.pdf

CSL INTERNAL / ILLUSTRATIVE MODELLING

[1] Illustrative modelling based on publicly available NHS data. Indicative figures only; Trust-specific validation recommended.

[8] CSL Group internal data (Q4 2025).