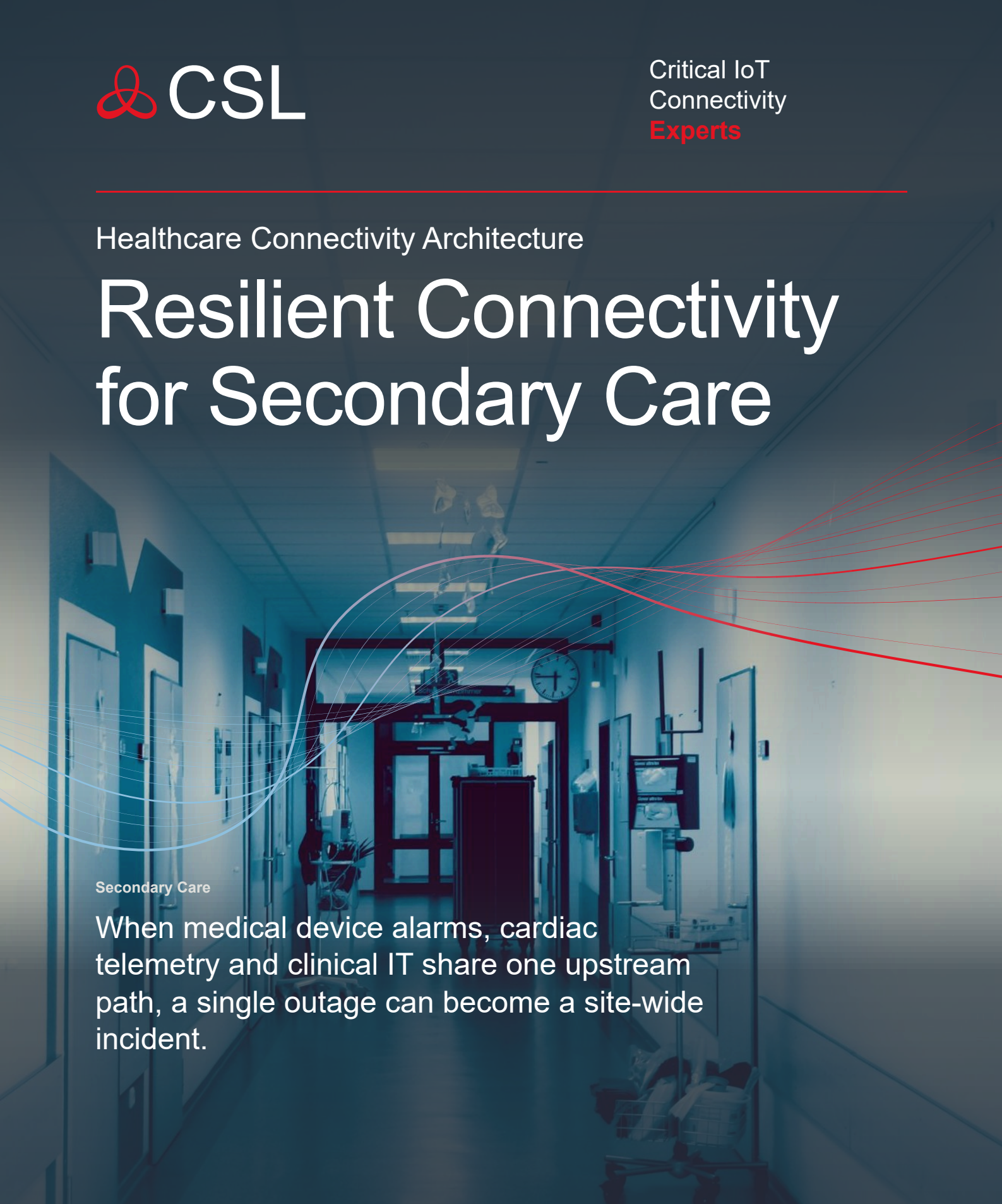
CSL

Critical IoT Connectivity **Experts**

Healthcare Connectivity Architecture

Resilient Connectivity for Secondary Care



Secondary Care

When medical device alarms, cardiac telemetry and clinical IT share one upstream path, a single outage can become a site-wide incident.

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

Version
4.2

Edition
April 2026

Multiple domains | One shared dependency | A resilient design response

Contents

1. Multiple Networks, One Hospital 3

Why multiple domains, not one network? 4

One estate. Multiple domains. One avoidable failure point. 5

2a. Clinical IT & Connected Medical Devices 6

2b. Estates, Life Safety & Building Systems 7

3. The Architecture Gap 8

4. Compliance & the Regulatory Landscape 10

5. Implementation Form Factors 12

6. Next Steps 15

Beyond the Hospital: Community & Home Connectivity 18

Appendix B: Planning Model 19

Appendix C: OT & Life-Safety Layer Diagram 21

Appendix D: Medical Technology Layer Diagram 22

About CSL Group 23

About this printing 24

Sources & notes 25

Figures

Figure 1: Ward telemetry vs life-safety signalling 5

Figure 2: Single-core multi-RAN vs CSL DualCore multi-core 9

Figure 3: One managed cellular architecture can serve both RPM and a third-party telecare ARC 18

Figure 4: OT & life-safety connectivity layer 21

Figure 5: Medical technology connectivity layer 22

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.

Many NHS organisations connect through national networks: the Health and Social Care Network (HSCN) in England, and the Scottish Wide Area Network (SWAN) in Scotland, which connects 22 NHS Scotland boards[1]. Within hospitals, the local networks that connect to HSCN and SWAN are designed around clinical IT.

The design question is whether every other domain should inherit the Trust WAN by default. Where a domain does, the shared failure point should be documented and, if the residual risk is unacceptable, separated.

A separate path also limits what a cyber incident can reach: if ransomware compromises the Trust network, the alarm pathways carried on that path may remain available, provided routing, authentication, monitoring and downstream dependencies are independently maintained. Alarm pathways are the routes that carry a medical device alarm, a telecare alarm, a telemetry feed, a nurse call or a lift alarm call to the people who respond.

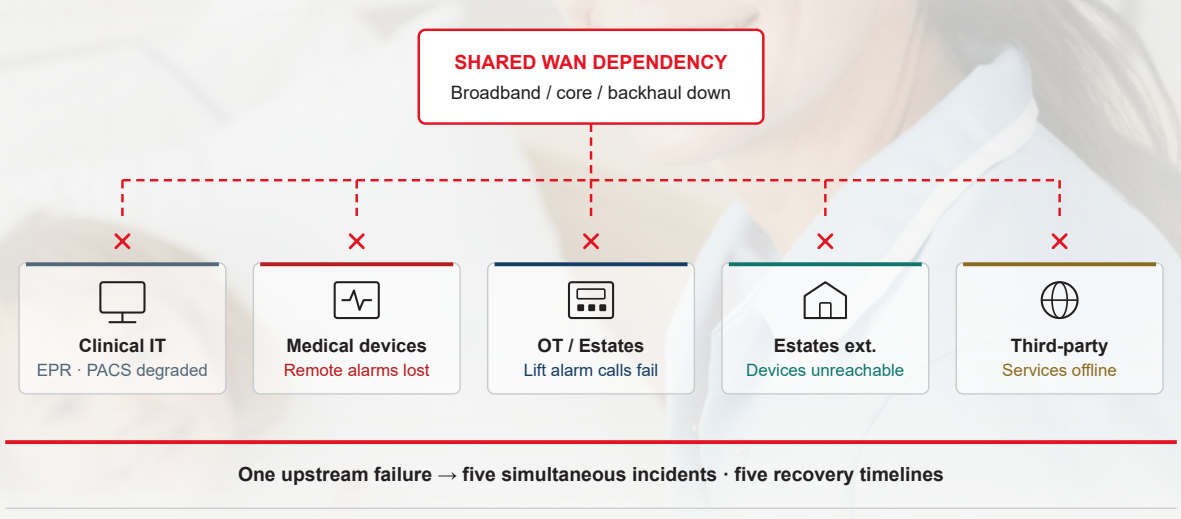
What a shared outage looks like

Where multiple domains share an upstream path, a single failure can create concurrent incidents across otherwise separate services: loss of telemetry visibility, failed clinical alarm transmission, interrupted estates signalling and reduced access to clinical platforms such as the electronic patient record (EPR). Each then needs its own team and procedure to restore it (page 4).

Where the services concerned depend on the external path, a cardiac alarm may not reach a remotely hosted central station and a lift alarm call may fail to connect.

Fire and security alarm signalling is outside the scope of this paper: it is fitted by CSL's accredited installer partners and by large system integrators, and carried to alarm receiving centres (ARCs) by CSL's alarm signalling products and services (page 14).

A planning model in Appendix B shows how a Trust can size the exposure of a cardiac monitoring fleet that shares a common upstream WAN[2]. The inputs are fleet size, outage frequency, recovery time, the share of device-hours without a remote alarm path that an independent path removes, that path's own outages and the cost of such a device-hour. Each is either an illustration the Trust replaces or a figure it supplies, and the cost per device-hour is always the Trust's own, because the paper makes no estimate of cost or harm. The worked example is on page 19.



Why multiple domains, not one network?

The diagram on page 3 shows what happens when the outer domains, meaning every domain other than clinical IT, inherit a shared upstream path. Virtual local area networks (VLANs) and other lateral segmentation separate traffic on the local network but leave the ***upstream*** dependency shared, so that dependency still has to be documented, separated or explicitly accepted.

Different owners

Trust IT, clinical engineering and estates are separate teams, each with its own systems and change process.

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 cardiac telemetry alarm that does not reach the monitoring station or a lost picture archiving and communication system (PACS) connection in radiology.

Different recovery timelines

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

NHS incident context: shared suppliers and systems

Recent NHS incidents show IT failures reaching many services at once. In June 2024, a ransomware attack on Synnovis, a pathology services provider, significantly reduced its capacity to process tests, with the greatest impact in south-east London. By late September NHS England's London region had reported provisional figures of 10,152 postponed acute outpatient appointments and 1,710 postponed elective procedures at the two most affected trusts[3]. In July 2024, NHS England reported that a global IT outage and an issue with a GP appointment and patient record system were causing disruption in the majority of GP practices. The statement adds that paper records and handwritten prescriptions were used as contingency measures[4]. In July 2025, Gloucestershire Hospitals reported IT disruption from a server issue, not a cyber incident[5]. Earlier, the August 2022 ransomware attack on Advanced was reported to have disrupted NHS 111 and left healthcare staff unable to access patient records[6].

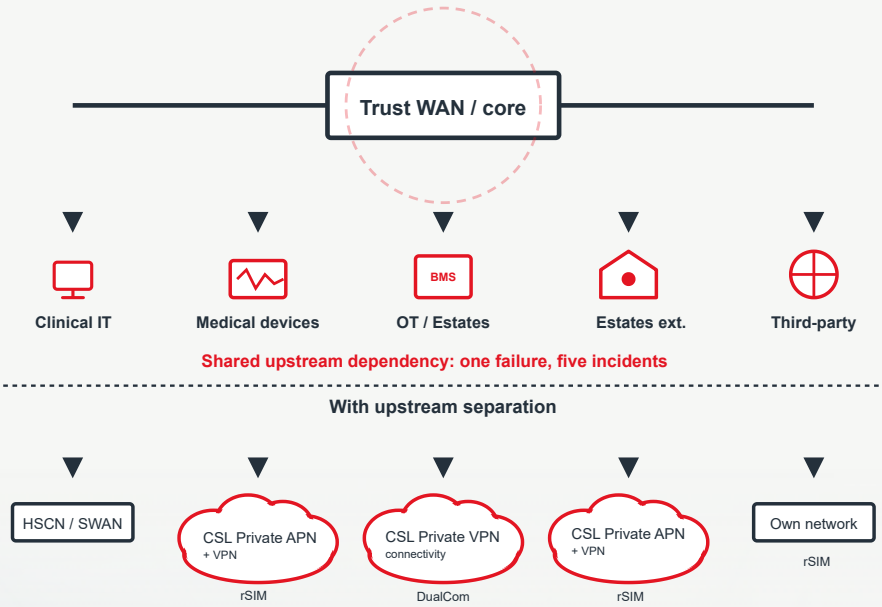
These incidents, however, primarily affected clinical IT systems, and where they exposed a shared dependency it was a supplier, service or system rather than a circuit. Where alarm pathways and life-safety systems share an upstream path with clinical IT, the circuit is the shared dependency, and one failure on it can reach every service it carries, even where no record lists it as such. A failure of alarm delivery on that path is also harder to detect. A failed EPR is generally visible to its users, whereas a cardiac alarm that does not reach a hosted monitoring station may produce no error message at all, unless that path is supervised. Supervision of the connection, such as a periodic heartbeat, shows that the path is up; showing that an individual alarm arrived needs an acknowledgement or delivery record for that alarm from the receiving platform.

Separately, a 2025 thematic review by the Health Services Safety Investigations Body (HSSIB) found that EPR systems could contribute to the risks of patient care being missed, delayed or incorrect. It also highlighted challenges with hardware and Wi-Fi availability in clinical environments[7]. A 2024 BBC Freedom of Information (FOI) investigation reported 126 instances of serious harm linked to IT issues across 31 trusts[8]. The concern is therefore wider than cyber events: it extends to functional availability at the point of care.

For the board: document where the external failure point is shared, where it is separated and who has accepted the residual risk, before a single failure reaches several governance domains at once.

One estate. Multiple domains. One avoidable failure point.

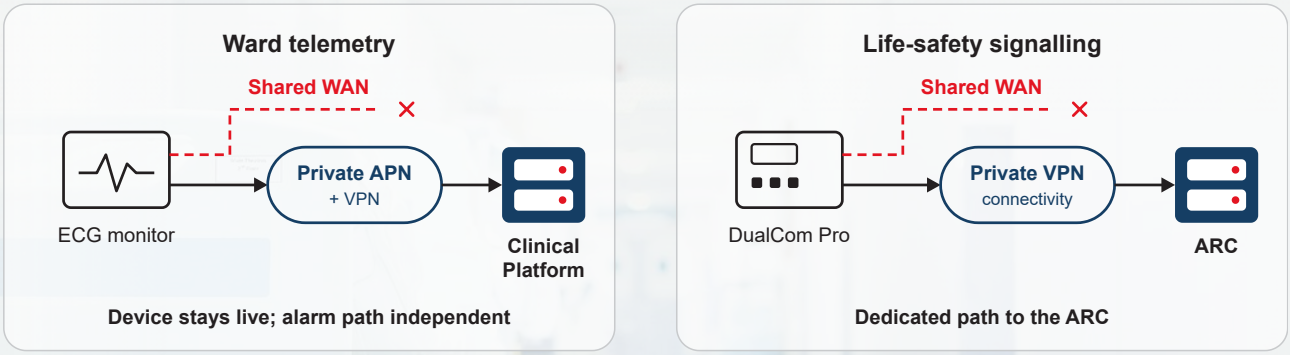
Shared dependency risk



The diagram shows which pathways still fail together when a shared WAN or hosted core is lost, whatever VLANs separate them on the local network.

A clinical alarm that is not delivered is a different incident from IT downtime

Different consequence



Same outage, different consequences, so the architecture should treat them separately.

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

For connectivity planning: a clinical IT outage triggers known workarounds, whereas a clinical alarm that is not delivered may go unnoticed until the response it should have prompted does not happen. Both can follow from one WAN failure: staff generally see an EPR failure and move to paper contingency, while the central station has no sign that a cardiac alarm was raised.

2a. Clinical IT & Connected Medical Devices

Hospital networks are designed around clinical IT. Medical devices add alarms that depend on the same upstream path wherever they report to a platform off the ward.

EPR / PAS & PACS

Where the EPR or the patient administration system (PAS) is hosted off site with no other path or offline copy, a WAN outage removes access to the hosted system. Remote radiology reporting stops where images are read over that WAN. 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 runs across CCU, ICU and telemetry wards. Where the central station is on the ward network, bedside units and station can continue together during a WAN outage. An alarm or telemetry workflow that depends on an external path (a hosted station, a messaging service, review off site), however, is lost with the WAN. An alarm raised but not received is a patient-safety risk.

Infusion pumps & syringe drivers

Smart pumps deliver precise drug doses across ICU, oncology and surgical wards. Dose-error and occlusion alarms are safety-critical and sound at the pump; the WAN carries them only where the pumps report to an alerting platform hosted off site. An outage removes only the remote view, and the ward's hazard log can record whether staff rely on that view or on the pump's alarm.

Mobile & untethered devices

This group includes ambulatory ECG holters, infusion pumps in transport and paramedic handover devices. These may move beyond reliable ward Wi-Fi coverage or may not be approved for the Trust wireless network. The right path therefore depends on device design, workflow and local assurance; for some, managed cellular is the primary and sometimes sole data path.

Risk

A medical device may keep working locally during a WAN outage while an alarm or telemetry workflow that depends on the shared WAN stops. An independent upstream path reaches a device through its own cellular module or a gateway on the ward network, such as CSL Outpost. Which route a device can take depends on what its manufacturer supports and on clinical safety approval.

Implementation example: CSL DualCore rSIM

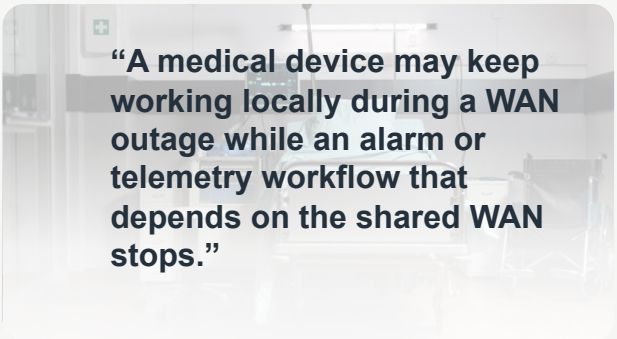
rSIM® is a SIM replacement for medical devices that already have a cellular module. Alerts sent over that module leave the site on the cellular network rather than the Trust WAN. With rSIM, logic on the SIM switches to a second operator core when its configured tests show that the active path has lost service. Firmware impact is minimal in most deployments, integration is usually through device configuration, and CSL works with device manufacturers to assess each device before wider rollout[9]. The device manufacturer should confirm that it supports the device's use with the replacement SIM[10].

How it works: rSIM delivers the CSL DualCore® architecture. One SIM holds two independent multi-network roaming profiles, on two independent core networks, and the failover decision is made on the SIM rather than in device firmware or in the network. The CSL DualCore architecture requires Private APN (access point name) routing and an encrypted connection on both paths.

For in-hospital devices: the device can stay on the ward LAN while its own cellular module, fitted with rSIM, provides an independent upstream path, subject to original equipment manufacturer (OEM) approval and local integration architecture. **For community and home devices with a cellular module:** rSIM is the primary connection, not a backup.

Implementation example: CSL Outpost

CSL Outpost is managed multi-bearer connectivity that combines up to four active mobile connections into one link, with satellite or fixed line incorporated where needed[11]. It suits a ward where several devices need independent upstream connectivity. CSL configures the link for each location, and manages and monitors it.



"A medical device may keep working locally during a WAN outage while an alarm or telemetry workflow that depends on the shared WAN stops."

2b. Estates, Life Safety & Building Systems

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

Lift alarms

BS EN 81-28 covers trapped-passenger alarm communications[12]. A lift alarm that signals over a public switched telephone network (PSTN) line needs a new path, because those lines are being switched off. A replacement that shares the clinical WAN, however, introduces dependency on infrastructure the estates team does not control. VoiceLink (page 13) is one option for replacing the PSTN line, subject to lift and alarm supplier design and local assurance.

BMS, CCTV & access control

Building management systems (BMS), CCTV and access control serve theatre air handling, pharmacy environmental monitoring, perimeter security and controlled entry. If BMS shares the clinical WAN, an IT change window can affect environmental control without warning.

Medical gas & water safety

Health Technical Memoranda (HTM) 02-01 and 04-01 provide for pipeline pressure alarms and for temperature monitoring to verify Legionella control[13,14], and estates teams usually run both. A separate estates path is therefore often easier to assure than a shared clinical IT path.

Implementation example: DualCom Pro

DualCom Pro provides dedicated signalling for fire and security systems to third-party ARCs (page 14).

Implementation example: CSL Outpost

BMS, CCTV, access control, nurse call, medical gas and water safety monitoring can all connect through one CSL Outpost link, the managed multi-bearer connectivity described on page 6. The link uses private networking and encrypted traffic, with satellite or fixed line incorporated where the site needs them.

What this means for Trust IT: estates pathways on their own upstream path are less exposed to clinical network maintenance and outages. The dependencies they keep, such as power and the site itself, nevertheless need to be recorded.



“A lift alarm that signals over a public switched telephone network (PSTN) line needs a new path, because those lines are being switched off.”

3. The Architecture Gap

Why does the upstream path matter?

When a medical device sends alarms over the ward LAN or hospital Wi-Fi to a platform or ARC reached through the WAN, that traffic shares the clinical WAN and broadband. When broadband fails, the remote alarm path fails with it, while the device and its local alarms can keep running.

Moving that traffic to a cellular path takes it off the clinical WAN, but not off every shared dependency, because access through several radio access networks (multi-RAN) can still depend on a **single hosted core**. Several networks sharing one mobile virtual network operator (MVNO) core give radio diversity but not core diversity: if that core fails, the alarm path is lost on all of them[15].

For high-consequence clinical and operational pathways, CSL treats **core independence** (two independent operator cores with autonomous failover between them) as a resilience requirement, and it should be explicitly assessed.

CSL requires private data paths on both cores, not only on the primary. A solution that routes alarm and telemetry data through a Private APN on one operator but falls back to public internet routing on failover does not meet the CSL DualCore requirement for private routing on both paths. CSL does not accept such a fallback for life-critical data, except as a planned and agreed short-term measure for connecting vital calls in an extreme outage. Both paths should use Private APN routing and 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 and telemetry pathways. A separate path reduces that exposure where its routing shares nothing with the Trust WAN. Two further properties keep it private: Private APN routing keeps the traffic off the public internet, and VPN encryption protects it on both routes. Each should be confirmed for the deployment, not assumed. The device, the receiving platform, the application and its credentials remain shared dependencies and are assessed on their own. The question is not whether cellular is as secure as HSCN; it is whether the same upstream dependency should carry clinical IT as well as higher-consequence life-safety, alarm and telemetry pathways.

In-building signalling resilience

Thick walls, basements, MRI-shielded rooms and lift shafts leave areas without usable Wi-Fi coverage. A cellular upstream path is independent of indoor Wi-Fi infrastructure. Because dense construction can also attenuate cellular signal, pre-deployment site surveys find the coverage gaps, and external antenna options are planned from their results.

Satellite sites and secondary buildings

Secondary buildings and outlying sites, away from the main hospital, often have unreliable broadband. A managed cellular router can provide failover for EPR, prescribing and records.

Broadband-dependent devices

Some connected devices rely on domestic or site broadband with variable quality, no formal service level agreement (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 path, independent of that broadband, with defined service levels.



3. The Architecture Gap (continued)

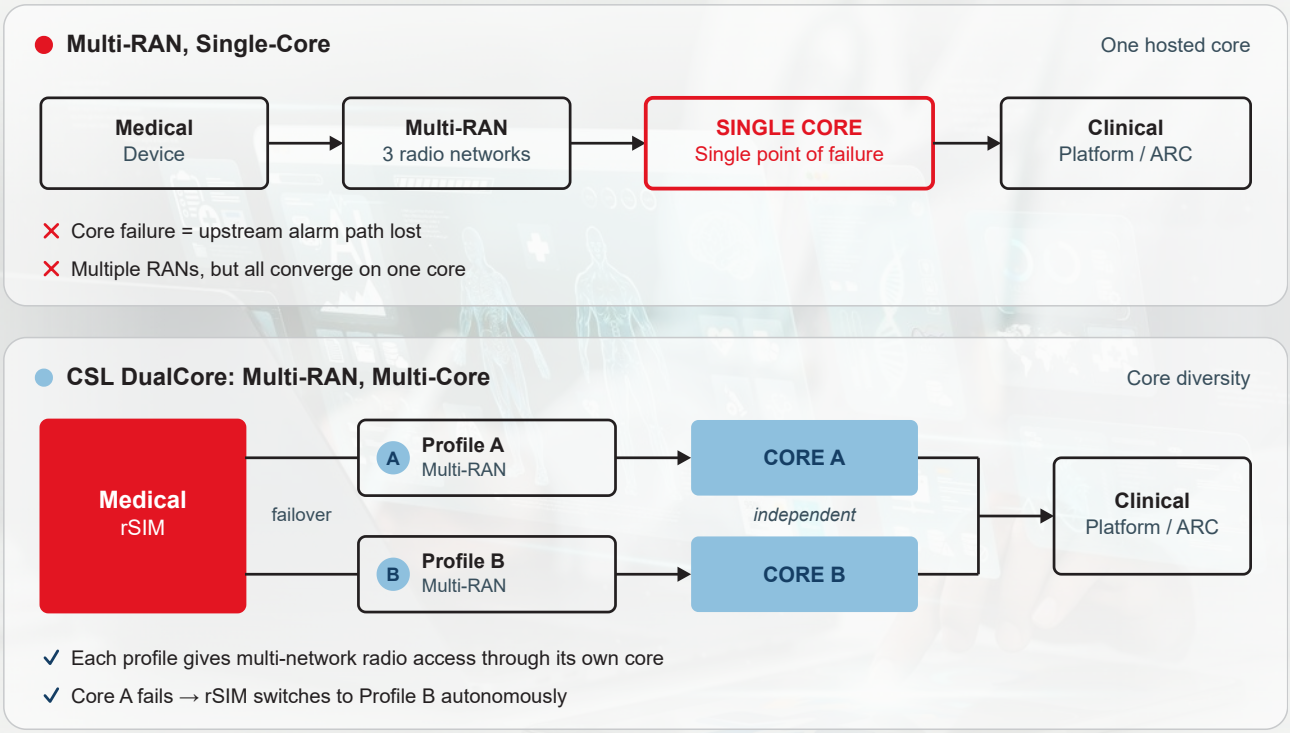


Figure 2: Single-core multi-RAN vs CSL DualCore multi-core. With independent operator cores, a failure confined to one core does not affect the other. Whether the other path stays in service also depends on its access network, its backhaul and the infrastructure beyond the core.

"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 clinical alarms. 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 takes alarm and telemetry delivery off the Trust WAN, so a degraded WAN no longer delays the alarm. Whether the alarm arrives within the required window, however, still has to be shown by testing the independent path.

Clinical IT

Emergency break-glass backup

When the Trust WAN fails completely, a CSL Outpost link can provide emergency backup connectivity for essential clinical services: EPR access, prescribing and discharge workflows. It carries them over private networking with encrypted traffic, independent of the failed broadband or HSCN path. That use has first to be configured and tested for the site. Clinical services then share the CSL Outpost link with alarm and telemetry traffic, so the hazard log should record that shared link.



4. Compliance & the Regulatory Landscape

The architecture gap, an alarm and telemetry path that shares the clinical WAN or a cellular path that depends on one operator core, is a governance question as well as a technical one. The frameworks on these two pages are the ones to check a shared path against, and upstream separation can help evidence each.

Cyber assurance

Security & cyber resilience

A logically and operationally separate path, such as CSL's Private APN infrastructure, may keep alarm and telemetry pathways running during a cyber incident on the Trust network, where its routing, authentication and monitoring are independent of the Trust WAN (page 8). A path of this kind supports evidence under National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) principle B5 (Resilient networks and systems). The device, platform, application and credentials, however, remain shared dependencies.

Data security

NHS DSPT (CAF-aligned, 2025 to 2026)

Version 8 of the Data Security and Protection Toolkit (DSPT), for 2025 to 2026, aligns to CAF v3.4. *(NCSC has since published CAF 4.0; see note 16.)* CAF principle B5 states in outcome B5.b that *"systems are appropriately segregated and resource limitations are mitigated".* Its achieved indicator names single network paths among the resource limitations to identify and mitigate. A shared upstream path should therefore be assessed against that indicator, and a multi-domain model can make single network paths and gaps in separation explicit so that they can be mitigated[16].

Health IT standards

DCB0129 / DCB0160: Clinical Safety

Where a connected device, platform or integration is a health IT system within the scope of the standards, DCB0129 sets clinical risk management requirements for its manufacturer and DCB0160 for the health organisation deploying it. Where alarms or telemetry depend on a network path, connectivity loss should be considered as a foreseeable hazard. An independent upstream path can be one control for that hazard, subject to local clinical safety assessment[17].

Care regulator

Care Quality Commission (CQC) Regulation 12

Regulation 12 (Safe care and treatment) sets duties to assess the risks to service users, to mitigate them so far as reasonably practicable and to ensure that equipment used in care is safe. It does not name medical device connectivity[18]. Where a provider's risk assessment does include loss of device connectivity, however, an independent upstream path can support the record of mitigation.



"Systems are appropriately segregated and resource limitations are mitigated."

NCSC Cyber Assessment Framework, outcome B5.b

4. Compliance & the Regulatory Landscape (continued)

Device regulator

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. The 2024 amending regulations for Great Britain came into force on 16 June 2025. The Medicines and Healthcare products Regulatory Agency (MHRA) describes the new post-market surveillance requirements as "generally more stringent than before"[19]. They apply to devices placed on the market or put into service in Great Britain from that date. Where a manufacturer gathers surveillance data from connected devices in service, a resilient connection makes gaps in that data less likely.

Supplier assurance

NHS Procurement: DTAC

NHS England introduced an updated Digital Technology Assessment Criteria (DTAC) form on 24 February 2026, and the previous form should not be used from 6 April 2026[20]. DTAC is scoped to software-based digital health technologies. Where a software product in scope sends alarms over a network path, the Trust should ask its supplier how that path is provided and supervised.

Deployment records

Clinical Safety Documentation

Where a deployment falls within DCB0160, the deploying organisation should update its clinical safety documentation through its established process, such as its hazard log and Clinical Safety Case Report. A separated pathway still needs that clinical safety case work, cyber assurance and local governance, and the independent upstream path becomes one of the controls they record.



5. Implementation Form Factors

CSL DualCore architecture can be delivered through several products. Any deployment specified to deliver it, whatever its form factor or device category, is built to three design principles:

Principle 1 Independent operator cores: the two paths run through operator cores independent of each other, not several radio networks sharing one core.

Principle 2 Autonomous switching: SIM- or device-resident switching between the cores, with no wait for a platform instruction. At scale, reversion should be staggered.

Principle 3 Private routing on both paths: Private APN + VPN encryption applies on primary and failover, not only one.

For hospital alarm and telemetry pathways, the design in this paper also keeps their traffic off the clinical WAN. The choice of deployment model depends on device type, site topology and local governance, and some assets may keep a shared path where the risk is documented and a named owner has accepted it (page 17 gives examples). Among the examples below, rSIM and a CSL DualSIM® Router configured for core independence implement the CSL DualCore architecture where a deployment is built to all three principles. A Trust should therefore check each deployment against them. A router failing over from fixed broadband to cellular gives access-path diversity instead, with one operator core on the cellular leg. CSL Outpost is managed multi-bearer connectivity that complements the CSL DualCore architecture, and the independence of its underlying paths is confirmed for each deployment. The three remaining examples are VoiceLink, for lift alarms; CSL Signal Analyser 2, for surveying mobile coverage at each installation point; and DualCom Pro, for fire and security systems.

Per-device separation

Deployment context: upstream signalling for hospital telemetry and infusion alarms; primary connectivity for continuous glucose monitors, continuous positive airway pressure devices, Hospital at Home kits and community remote patient monitoring (RPM) devices.

rSIM is a SIM replacement for medical devices that have a cellular module, and CSL assesses each device with its manufacturer before wider rollout. For in-hospital devices, rSIM provides an independent upstream alarm and telemetry path through that module. The device can remain on the ward LAN while its outbound signalling takes the independent path, as page 6 describes. For community and home devices, rSIM is the primary resilient connection.

Site-level failover

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

A CSL Router adds a mobile backup to a site's fixed broadband, or provides a primary cellular path for sites without reliable fixed connectivity. CSL configures and manages the router. Where it fails over from fixed broadband to cellular, the router gives the access-path diversity described above; a CSL DualSIM Router configured for core independence gives the site two independent operator cores.

rSIM **rSIM**
Device-level resilience



RTR **CSL Router**
Fixed broadband with cellular failover



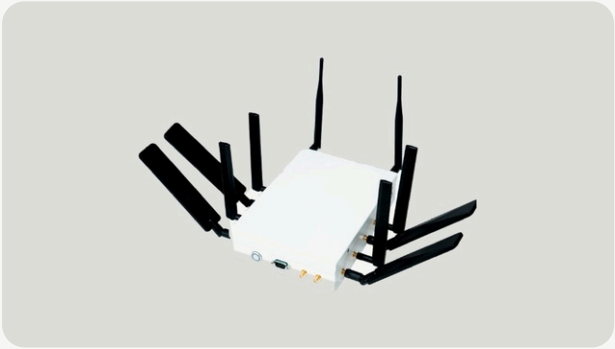
5. Implementation Form Factors (continued)

Multi-service aggregation

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

At sites where several outer domains need an upstream path independent of the clinical WAN, CSL Outpost gives them one managed link (page 6), with satellite or fixed line incorporated where needed. It carries upstream medical device signalling, nurse call and estates monitoring traffic over that link, and CSL configures it for the site, manages it and monitors it. Fire signalling to the ARC stays on DualCom Pro. When the Trust WAN fails completely, the same link can provide break-glass connectivity on the conditions given on page 9.

OUT **CSL Outpost**
Hospital edge aggregation



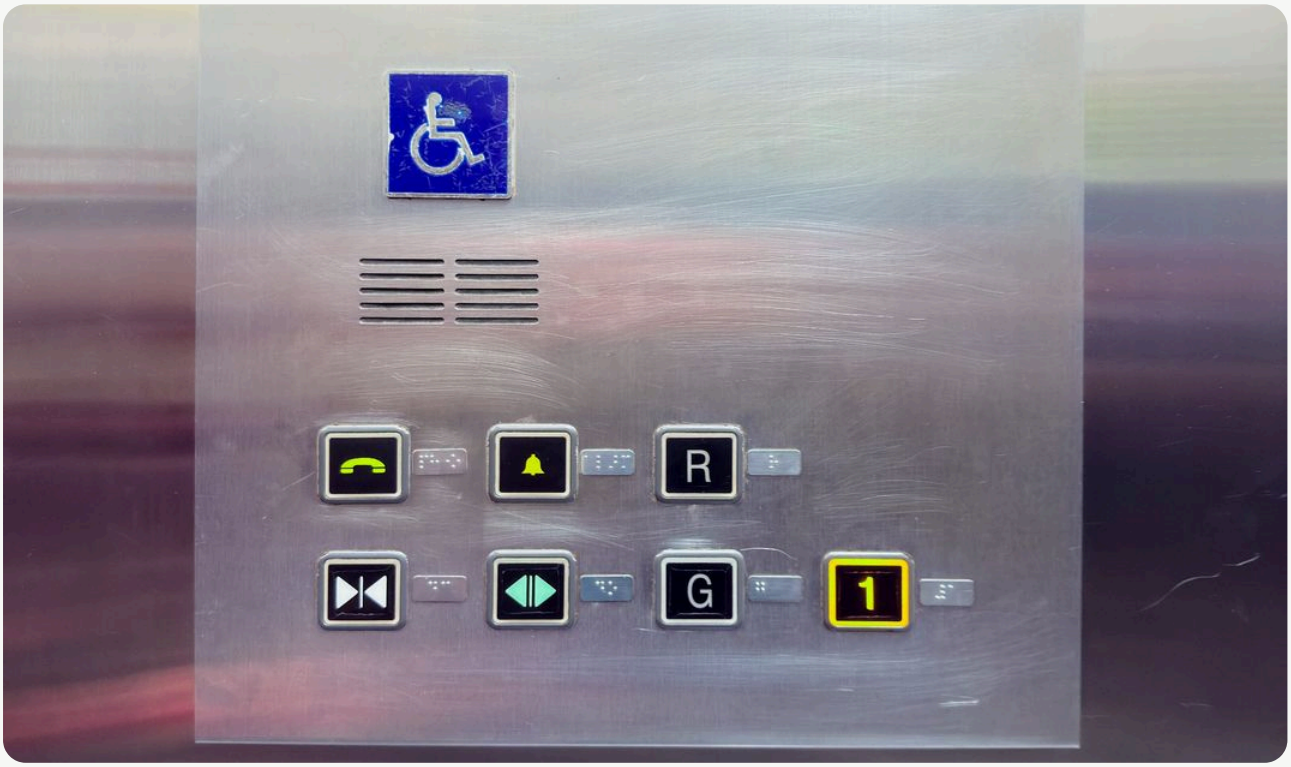
Lift alarm voice path

Deployment context: lift alarm panels whose PSTN line needs replacing, with BS EN 81-28 covering the remote alarm.

VoiceLink is one option for that replacement: a cellular voice and data gateway that carries trapped-passenger alarm calls on the 4G network as voice over LTE (VoLTE), without using the clinical WAN or broadband[21].

VL **VoiceLink**
PSTN replacement for lift alarms





5. Implementation Form Factors (continued)

Site survey

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

CSL Signal Analyser 2 is a handheld survey tool that identifies the strongest available mobile network at each installation point. It shows the highest signal strength reading for each available network and exports reports for documentation and sign-off. Device placement in lead-lined rooms, basement plant areas and shielded zones can therefore be decided from measured signal.

CSL Signal Analyser 2
Pre-deployment site survey



Dedicated alarm path

Deployment context: DualCom Pro serves hospital fire panels, medical gas manifold alarms and security systems.

It is dedicated signalling hardware that carries alarms from these systems to third-party ARCs. CSL connects to more than 270 ARCs across Europe and does not operate them.

DC

DualCom Pro
Life-safety and ARC signalling





6. Next Steps

Clinical IT belongs on the Trust WAN, but the outer domains often inherit that same path by default. A Trust's next step is therefore to find where a common failure point creates unacceptable risk and to decide, pathway by pathway, whether to separate that dependency or accept it.

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 and 2:** a managed connectivity partner can provide a dependency mapping workshop covering device estate audit, shared-path identification and an upstream risk register.

3. Confirm governance owners across CIO, CCIO, clinical safety officer (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 in a controlled window, with downtime procedures in place, before relying on it.

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

Where separation is most likely to matter first

High-acuity monitoring and alarm workflows (cardiac telemetry, vital signs) · infusion and drug delivery pathways (patient-controlled analgesia, syringe drivers) · 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. For network planning beyond these pathways, a Trust can draw on NHS England's Networks and Connectivity Centre of Excellence, which "supports NHS organisations to have resilient and efficient networks and the required level of fixed and wireless connectivity across all sites and into the community"[22].

Pre-deployment checklist

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

☐ **Private APN on both cores:** for pathways built to the CSL DualCore design principles (page 12), end-to-end VPN encryption and no public internet breakout on either path.

☐ **Clinical safety hazard log reviewed:** connectivity loss logged as a hazard (page 10).

☐ **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:** the routing, authentication and monitoring of the independent path are independent of the Trust WAN, and its traffic does not traverse the public internet. Any part of the device-to-platform path that still uses hospital infrastructure, such as the ward LAN between a device and its gateway, is recorded as a retained dependency.

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

Start here: where they signal over the shared path, high-acuity telemetry (cardiac monitors), infusion pumps and lift alarms carry the highest consequence of its failure. Begin with one pathway, validate the architecture with the device manufacturer and the clinical safety officer, then extend.

6. Next Steps (continued)

Governance & assurance responsibilities

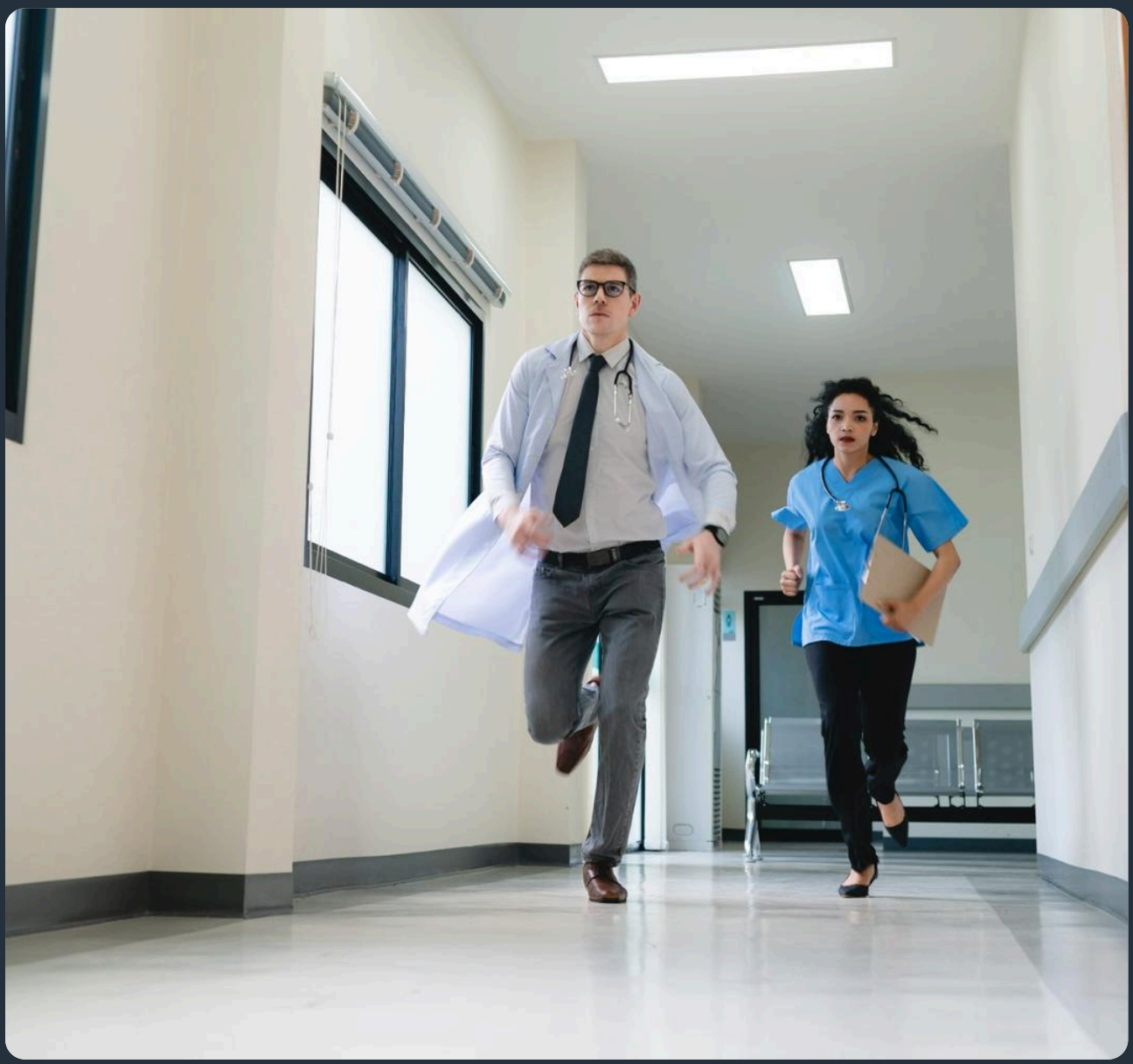
Trusts should ensure that clinical safety ownership remains with the responsible manufacturer (DCB0129) and deployer (DCB0160). Local risk acceptance, change control and cyber review should be completed before deployment, and supplier due diligence should cover connectivity, failover SLA and data handling.

“Local risk acceptance, change control and cyber review should be completed before deployment, and supplier due diligence should cover connectivity, failover SLA and data handling.”

Illustrative NHS deployment examples

Satellite site broadband resilience: a community hospital with a single broadband circuit and no HSCN connection loses EPR access during outages. A CSL Router adds cellular failover to that circuit, so that prescribing and discharge workflows can stay online.

Cardiac telemetry fleet: a Trust with more than 200 cardiac monitors across CCU, ICU and telemetry wards finds that the monitors’ alarms reach a hosted central station over the clinical WAN. Monitors on the ward LAN can send that traffic upstream through CSL Outpost, and those fitted with a cellular module can use rSIM instead. Neither route replaces the ward LAN, and rSIM is usually integrated through device configuration rather than a firmware change, once the manufacturer has validated the device.



6. Next Steps (continued)

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 point-of-sale systems can stay on a shared path where the clinical and operational risk is understood and documented, and a named owner has accepted it.

Procurement routes

Public sector frameworks open to NHS buyers, now run by the Government Commercial Agency, include mobile voice and data (RM6261) and network services with a lot for IoT and smart cities (RM6116)[23]. Estates and medical device connectivity need not therefore be bought through the clinical WAN contract. A Trust's procurement team should check each framework's scope and current status before use.

An on-campus network is an independent path only where its backhaul avoids the Trust WAN

Where a Trust runs a private 5G or neutral-host network on campus, it should establish whether that network's backhaul shares the Trust WAN before treating it as an independent path. CSL can discuss how such a network relates to the design principles on page 12.

Beyond the acute site: page 18 sets out how the operating context differs in community and home settings.

Contact CSL

Web: csl-group.com

Email: sales@csl-group.com

Phone: +44 (0) 1895 474 474

To scope an independent upstream path for a Trust's estate, CSL can hold an initial planning conversation.

"Not every connected asset requires full path independence."



Beyond the Hospital: Community & Home Connectivity

Beyond the hospital wall, as inside it, the aim is to give alarm and telemetry traffic an upstream path that does not depend on the general-purpose connection it would otherwise use. The operating context there differs, however: there is no managed WAN to separate from, no on-site IT team and no single commissioner.

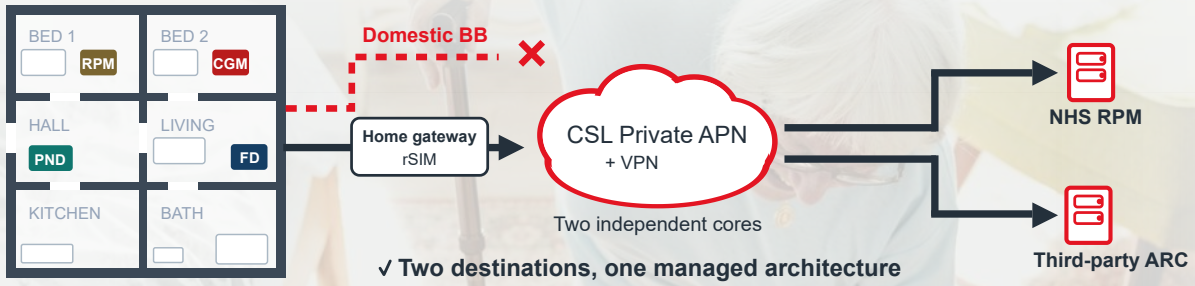


Figure 3: One managed cellular architecture can serve both RPM and a third-party telecare ARC. Remote patient monitoring and telecare alarm escalation need not depend on domestic broadband, whichever body commissions each service.

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

This paper covers the acute site

GP surgeries, remote clinics, Hospital at Home, remote patient monitoring and council telecare raise the same question of a shared upstream path, as does the PSTN switch-off. The paper's analysis is of the acute hospital site, so the paper covers those settings only on this page.



Appendix B: Planning Model

This appendix provides a hypothetical scenario model for planning and decision support only. The paper makes no estimate of outage cost or harm, and the model draws on no published claims or cost data; every input is either an illustration the Trust replaces or a figure it supplies itself[2].

For a 200-device cardiac monitoring fleet sharing a common upstream WAN, the model counts the device-hours in a year during which alarms have no remote path, and then deducts the share of those hours that an independent path removes. The Trust multiplies the gross device-hours by its own cost of a device-hour without a remote alarm path, built from clinical staff time on manual observation and activity delayed because alarms cannot reach their remote station. 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

Unavailable device-hours a year = Fleet × Outages/yr × Recovery hrs

Annual cost = Unavailable device-hours × Cost per device-hour (the Trust's figure)

Input	Value	Basis
Fleet size	200 monitors	Illustrative (CCU, ICU, telemetry wards)
Upstream outage events	3/year	Assumption; use the Trust's incident log
Mean recovery time	4 hours	Assumption; use the Trust's incident log
Cost per device-hour without a remote alarm path	Trust's own figure	Trust costing; components as listed above

Unavailable device-hours on the shared path: 200 × 3 × 4 = **2,400 device-hours/year without a remote alarm path**. The annual cost is those hours multiplied by the Trust's cost per device-hour.

With independent upstream path: if an independent upstream path removes an assumed 90 to 99 per cent of those device-hours, the residual from WAN outages falls to **between 24 and 240 device-hours a year**, and to 120 device-hours at a mid-range assumption of 95 per cent. Trusts should set the share removed based on local outage data and upstream path architecture.

The planning model is a simplified linear approximation. It treats every device-hour without a remote alarm path as equal, which a Trust may refine by weighting wards or pathways by acuity, and it assumes that WAN outages do not overlap. It also counts only hours of WAN outage. A Trust that moves alarms onto the independent path should therefore add that path's own outages while the WAN is working to the residual. Both kinds of outage are counted in device-hours: the hours each lasts multiplied by the devices it affects. The share removed takes account of the part of the fleet the independent path reaches and of any failure of that path during a WAN outage. Costs of recovering the WAN itself, such as supplier call-out, arise whether or not an independent path exists, so they stay outside the cost per device-hour.



Appendix B: Planning Model (continued)

How an independent upstream path works

In the CSL DualCore architecture delivered through rSIM, the modem registers on a mobile network using the SIM's active profile. Its traffic is routed through a Private APN, with a VPN tunnel that encrypts it on the way to the platform or third-party telecare ARC. The SIM holds the two roaming profiles described on page 6, on independent core networks. If the active profile's core fails, logic on the SIM detects the loss of service and selects the alternative profile, and the modem re-registers. Private routing and encryption apply on both paths, as Principle 3 sets out (page 12), and the same routing and firewall controls can be applied to each. For hospital alarm and telemetry pathways, the design in this paper also keeps both paths off the Trust network's routing. What they may still share, such as the device, the private routing beyond the mobile cores, the application, the platform at the far end and the credentials used to reach it, needs assessing on its own. The result is an alarm and telemetry path that can remain available when the hospital's own broadband or WAN is down, and when one operator core fails.

Managed reversion at scale

When a network recovers, displaced devices can attempt to reconnect within a short window, concentrating signalling load on it. CSL DualCore deployments at scale should include staggered reversion, a managed migration back to the primary path over a controlled window. For rSIM, CSL describes the return to the primary network as algorithmic[9].

Deployment pathways

rSIM swap SIM replacement for medical devices that have a cellular module, integrated as page 6 describes. Where a deployment confirms independent cores, and both rSIM paths have private routing and an encrypted connection, the CSL DualCore architecture is delivered at device level.

CSL Router Fixed broadband with cellular failover, CSL managed. The CSL DualCore architecture can be delivered for a site through a CSL DualSIM Router configured for core independence, with private routing and an encrypted connection on each route. The CSL Router replaces or supplements the site router where several device categories share a site.

CSL Outpost Managed multi-bearer connectivity that complements the CSL DualCore architecture, described on page 6. It can carry several device categories through one unit and works for a single site or a multi-site estate; CSL configures, manages and monitors it[11]. The independence of its underlying paths is confirmed for each deployment.



Appendix C: OT & Life-Safety Layer Diagram

This layer covers lift alarms, nurse call, medical gas monitoring, water safety, CCTV, access control, electric vehicle (EV) charging and BMS connectivity. In this illustrative design, a large hospital uses CSL products across four connectivity paths: DualCom Pro for fire and security signalling to the ARC, VoiceLink for lift alarm signalling, CSL Outpost for estates aggregation and a CSL Router for operational technology (OT) backhaul, each drawn separate from the clinical LAN and WAN.

Life safety + estates controls **Separate CSL paths** **Illustrative placement**

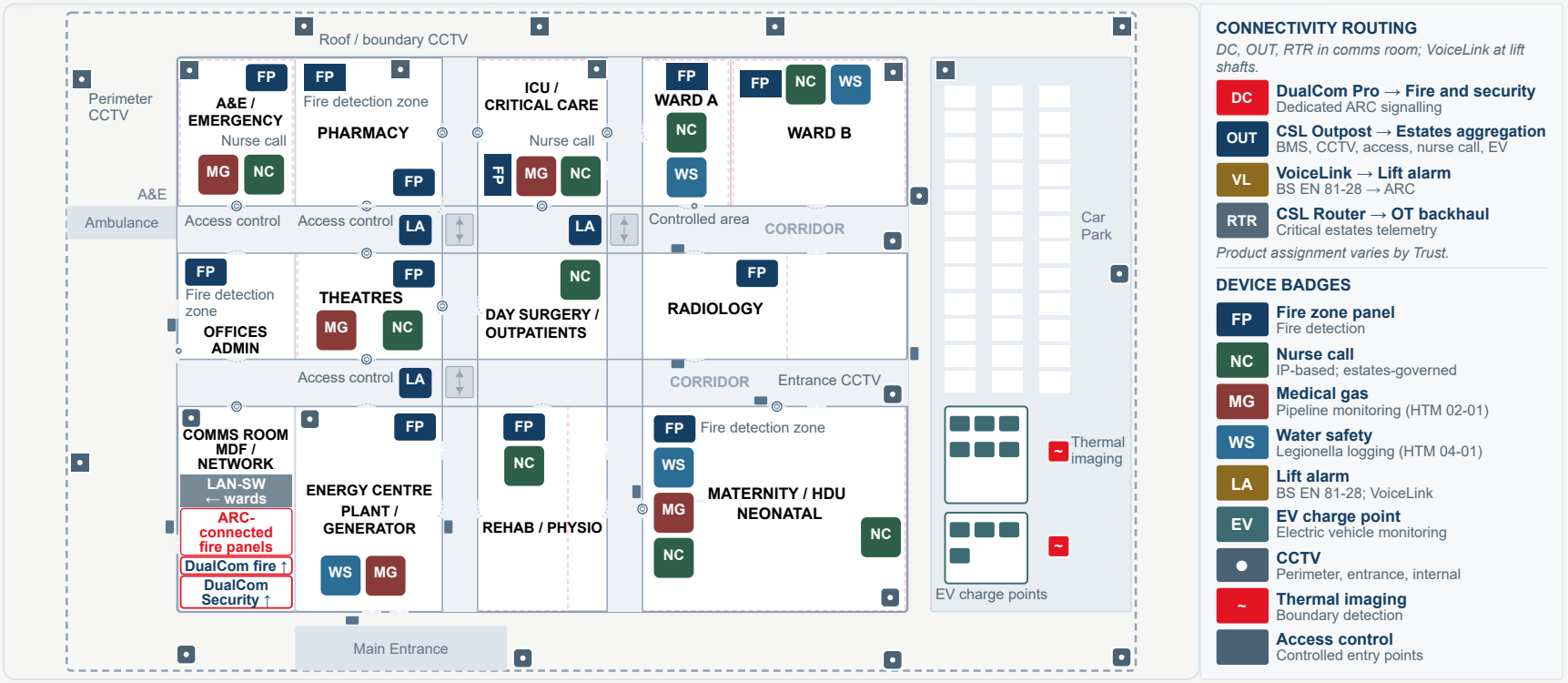
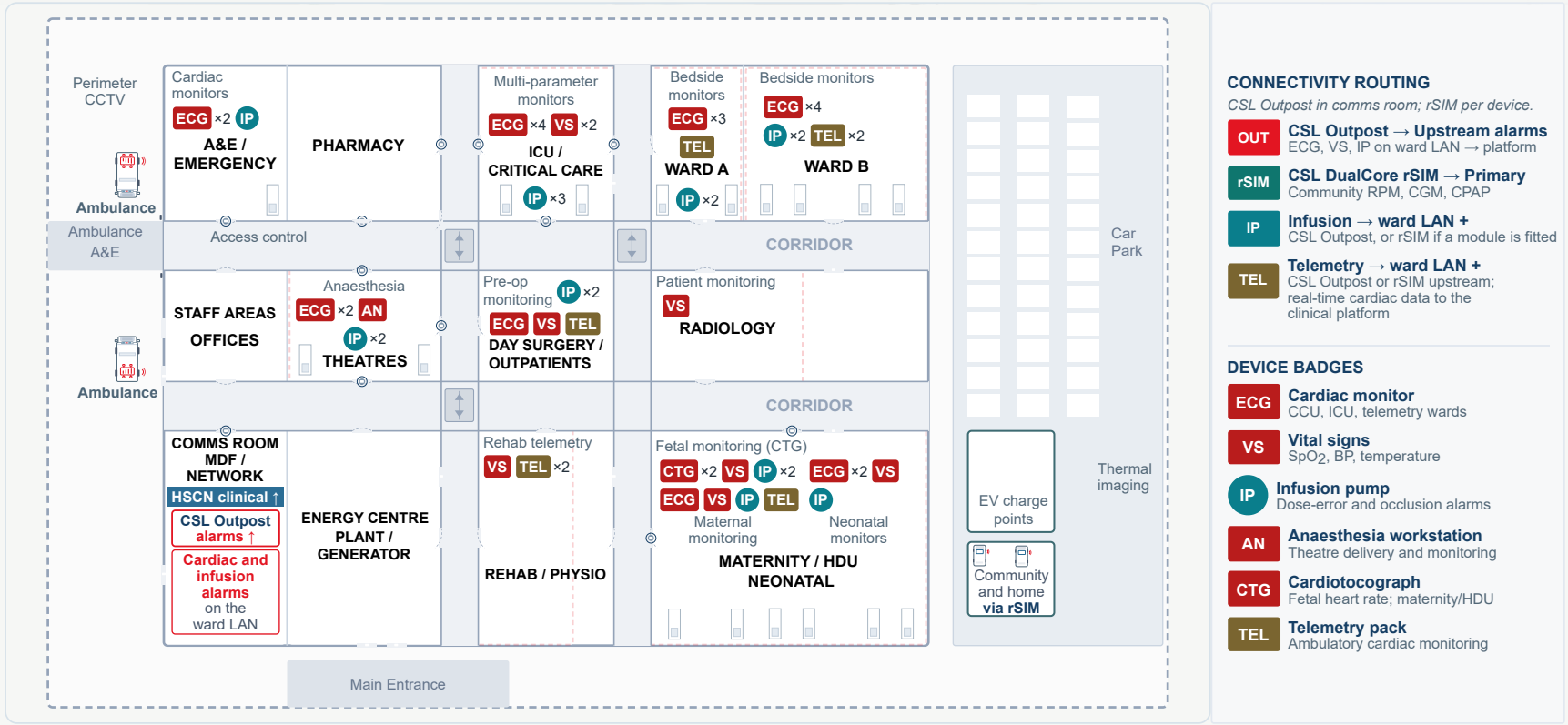


Figure 4: OT & life-safety connectivity layer. DualCom Pro carries signalling from the fire panels and security systems to the ARC. Estates systems (BMS, CCTV, access control, nurse call, medical gas, water safety, EV chargers) aggregate through one or more CSL Outpost units or CSL Routers. Lift alarms (BS EN 81-28) connect via VoiceLink as a cellular replacement for PSTN signalling. CSL Outpost provides private networking with encrypted traffic; the routing and encryption of the other paths are set for each deployment. Where a CSL unit sits in the comms room, its power and cooling are dependencies to record, as page 7 sets out. Actual product assignment varies by Trust estate.

Appendix D: Medical Technology Layer Diagram

In this illustrative design for cardiac monitors, vital signs, infusion pumps and RPM devices, in-hospital devices connect via the ward LAN, with independent upstream alarm and telemetry paths through CSL Outpost, or through rSIM where a device has a cellular module, separate from the clinical WAN. Community and home devices with a cellular module use CSL DualCore rSIM as the primary path.

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



CONNECTIVITY ROUTING

CSL Outpost in comms room; rSIM per device.

- **OUT** — **CSL Outpost → Upstream alarms** — ECG, VS, IP on ward LAN → platform
- **rSIM** — **CSL DualCore rSIM → Primary** — Community RPM, CGM, CPAP
- **IP** — **Infusion → ward LAN +** — CSL Outpost, or rSIM if a module is fitted
- **TEL** — **Telemetry → ward LAN +** — CSL Outpost or rSIM upstream; real-time cardiac data to the clinical platform

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 for cardiac monitors, vital signs, infusion pumps and RPM devices. Each badge stands for a device type, with the number of devices beside it where there is more than one. 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. CSL DualCore paths require private routing and an encrypted connection on both routes. CSL Outpost, managed multi-bearer connectivity that complements the CSL DualCore architecture, provides private networking with encrypted traffic.

About CSL Group

CSL Group is a UK and EU telecommunications company specialising in resilient connectivity for critical IoT, with more than 3.5 million active direct connections[24]. CSL provides connectivity for the outer domains, independent of the Trust WAN and its HSCN or SWAN connection, for medical devices and estates systems. Its network includes Private APNs through CSL's IoT core and private VPN connectivity to more than 270 ARCs across Europe[24]. At sites with unreliable broadband, a CSL Router can also provide failover for EPR, prescribing and records.

Key message: a shared upstream path is a risk a Trust can document and assess. Where clinical 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.

Evaluation criteria for upstream connectivity providers

Core architecture: Ask whether resilience is delivered through independent operator cores, each with its own 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: Establish how much each device's firmware has to change for the second path, who validates that change and what the manufacturer has to confirm. Each change brings clinical safety work and affects deployment timescale, OEM dependency and change-control burden.

Security and compliance posture: For pathways built to the CSL DualCore design principles, verify that both connectivity paths use Private APN with end-to-end VPN encryption and no public internet breakout. A path configured in that way supports evidence under CAF principle B5, and should also be checked against principles B3 (Data security) and B4 (System security).

Operational heritage: Assess whether the provider has a track record in life-safety and critical signalling, not only commercial IoT. Private VPN connectivity to alarm receiving infrastructure shows that a provider already carries signalling where connectivity failure has direct safety consequences.

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.

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

Scope & limitations

This paper presents an illustrative architecture model, and how it applies to a site depends on device type, OEM integration, local architecture and governance route. The multi-domain model is a decision framework for documenting where operational domains share a common external path; the Trust still carries out its own clinical safety and cyber assurance on any design. A Trust should validate the design for its own estate before procurement.

About this printing

Version 4.2 is a revised printing of the April 2026 edition, and its argument, the order of its numbered sections and its edition date are unchanged. Its claims keep their April 2026 evidence cut-off except where a note gives a later date, as the product descriptions, the company figures on pages 14 and 23 and notes 1, 22 and 23 do. The appendices keep the April edition's lettering, B to D, so that references to them still hold.

Appendix B. The appendix is now a planning model, which counts the device-hours a cardiac monitoring fleet spends without a remote alarm path. A Trust prices those hours from its own records, so the April edition's illustrative cost figures, drawn from NHS Resolution statistics and the National Cost Collection for 2024/25, are not included.

Incidents. The NHS incidents on page 4 follow their published accounts. The Synnovis figures, for example, are NHS England London's provisional counts of postponements at the two most affected trusts.

Regulation and standards. Pages 10 and 11 name the provision to check in each framework, and quote Cyber Assessment Framework outcome B5.b and MHRA's description of the post-market surveillance requirements in their own words.

CSL products. The product descriptions include the CSL DualSIM Router for core independence and the three design principles to which a CSL DualCore deployment is built. CSL Outpost is described as managed multi-bearer connectivity that complements CSL DualCore architecture.

Series and layout. The paper now stands on its own, without the series numbering of the April edition. It adds a contents page and sets some topics in sections 4 to 6 in a different order, and its page numbers therefore differ from those of the April edition.



Sources & notes

[1] NHS England Digital. *Health and Social Care Network*. Last edited 24 August 2026; page as read October 2026. Many NHS organisations have connected to HSCN. https://digital.nhs.uk/services/health-and-social-care-network NHS National Services Scotland. *SWAN contract award*. 24 April 2023; page as read October 2026. 22 NHS Scotland boards connected, with services to be enabled across over 6,000 sites and 94 public sector organisations. https://www.nss.nhs.scot/news/nhs-national-services-scotland-nss-awards-350million-swan-contract-to-bt-for-enhanced-public-sector-connectivity/

[2] Appendix B planning model: a linear scenario model whose inputs are illustrations the Trust replaces, or figures it supplies, from its own incident and cost records. The April edition's illustrative cost estimate drew on NHS Resolution statistics and the National Cost Collection for 2024/25. Indicative only; Trust-specific validation recommended.

[3] NHS England. *Synnovis ransomware incident* (3 June 2024). Services fully restored by December 2024. https://www.england.nhs.uk/synnovis-cyber-incident NHS England London. Update of 26 September 2024, the source of the postponement figures. https://www.england.nhs.uk/london/2024/09/26/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-26-september-2024/

[4] NHS England. *Statement on GP clinical system disruption during global IT outage*. 19 July 2024. https://www.england.nhs.uk/2024/07/response-to-global-it-outage

[5] Gloucestershire Hospitals NHS Foundation Trust. *IT disruption from 22 July*. 23 July 2025. https://www.gloshospitals.nhs.uk/about-us/news-media/press-releases-statements/it-disruption-22-july

[6] ICO. *Enforcement decision on Advanced Computer Software Group*. March 2025. The decision concerns the ransomware incident of August 2022. https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited

[7] HSSIB. *Electronic patient record systems: thematic review*. 2025. https://www.hssib.org.uk/patient-safety-investigations/electronic-patient-record-epr-systems-thematic-review

[8] 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. https://www.digitalhealth.net/2024/05/bbc-investigation-links-nhs-it-failures-to-patient-harm

[9] CSL Group. *rSIM documentation*: the solution page and the OEM article of 15 July 2026. As at October 2026. The solution page describes switching built into the SIM and algorithmic return to the primary network. The OEM article describes two independent core network profiles on one SIM and integration mostly through device configuration, and says CSL can demonstrate failover on sample devices before rollout. Solution page: https://www.csl-group.com/solutions/rsim/ OEM article: https://www.csl-group.com/blogs/why-oems-need-resilient-connectivity-built-into-the-product/

[10] Whether a device is supported with the replacement SIM is the manufacturer's decision, and its confirmation is the evidence to ask for.

[11] CSL Group. *CSL Outpost*. Solution page, as at October 2026. CSL Outpost bonds up to four mobile connections, plus satellite and fixed line where needed; CSL installs and configures the unit and monitors the service. https://www.csl-group.com/solutions/csl-outpost/

[12] *BS EN 81-28:2022*. Lift alarm signalling. https://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

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

[14] *HTM 04-01*. Water safety. https://www.england.nhs.uk/wp-content/uploads/2021/05/DH_HTM_0401_PART_A_acc.pdf

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

[16] Data Security and Protection Toolkit. *DSPT news*, 18 September 2025: "DSPT Version 8 is aligned to CAF version 3.4." Submission deadline 30 June 2026. Verify current deadline with NHS England. News: https://www.dsptoolkit.nhs.uk/News/161 Independent assessment guides: https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides NCSC. *CAF 4.0*. Published August 2025. CAF B5.b calls for systems to be appropriately segregated and for resource limitations, including single network paths, to be identified and mitigated. https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b5-resilient-networks-and-systems

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

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

[19] MHRA. *Post-market surveillance requirements for medical devices in Great Britain*. Introduction and scope: the 2024 amending regulations, in force from 16 June 2025. https://www.gov.uk/government/publications/medical-devices-post-market-surveillance-requirements/introduction-and-scope

[20] NHS England. *DTAC*. Updated form introduced 24 February 2026; the previous form should not be used from 6 April 2026. https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac

[21] CSL Group. *VoiceLink*. As at October 2026. VoiceLink converts PSTN calls to 4G VoLTE and is fitted with a CSL roaming SIM. https://csl-group.com/uk/voicelink

Sources & notes (continued)

[22] NHS England Digital. *Networks and Connectivity Centre of Excellence*. Last edited 10 September 2026; page as read October 2026. The Centre "supports NHS organisations to have resilient and efficient networks and the required level of fixed and wireless connectivity across all sites and into the community". https://digital.nhs.uk/services/networks-and-connectivity-centre-of-excellence

[23] Government Commercial Agency. *Procurement routes*. Status as at April 2026; verify current availability with a procurement team before use. HSCN DPS RM3825: https://www.gca.gov.uk/agreements/RM3825 GCA RM6261 Mobile Voice and Data Services: https://www.gca.gov.uk/agreements/RM6261 RM6116 Network Services 3 (now under GCA, formerly CCS; lot 3a covers IoT and smart cities, read October 2026) was extended to 17 July 2027: https://www.gca.gov.uk/agreements/RM6116 CCS became the Government Commercial Agency (GCA) on 1 April 2026: https://www.gca.gov.uk/news/introducing-government-commercial-agency

[24] CSL Group. Company figures as stated in October 2026: connection count, Private APN routing through its IoT core and ARC connectivity.



CSL

Healthcare Connectivity Architecture

Secondary Care

General enquiries

sales@csl-group.com

csl-group.com

+44 (0) 1895 474 474

This publication

First published April 2026 as version 4.1. Revised October 2026 as version 4.2; page 24 describes the revision. Product information and company figures updated October 2026. Evidence cut-off for all other substantive claims: April 2026, except where a note gives a later date.

Disclaimer This document is for general informational purposes only and does not constitute professional, medical, regulatory, financial or legal advice. Service-level commitments and SLA terms are contract-specific.

© 2026 CSL Group. All rights reserved. rSIM, CSL DualCore, CSL DualSIM and Critical Connectivity are registered trademarks of CSL (DualCom) Limited. The CSL mark is a trademark of CSL Group. Other names are the property of their respective owners and are used for identification only.