CLOUD GATEWAY

CONNECT

HEALTH CONNECT: CLOUD TO HSCN

SERVICE DEFINITION

V2.0
Issue Date: 10/07/2025
Commercial in Confidence

About this document

This document is designed to provide a straightforward, clear description of our **Cloud to HSCN** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Cloud to HSCN?

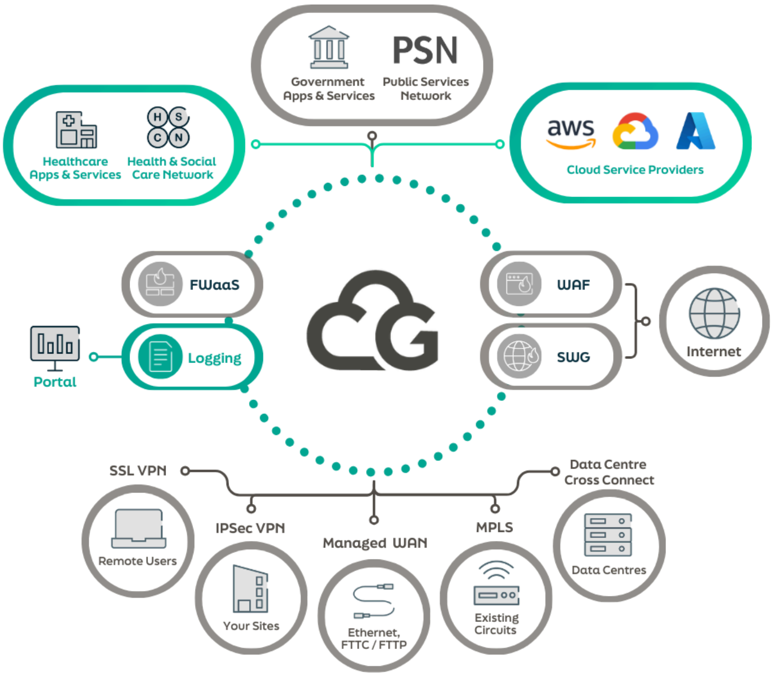
Cloud to HSCN provides connectivity between the Health and Social Care Network (HSCN) and your Cloud Service Provider (CSP). This service allows you to connect one cloud environment to the HSCN.

Cloud Connectivity can be deployed in two ways:

- A private connection via a dedicated on-ramp through our UK data centre presence
- An IPSec VPN connection deployed over the internet

Traffic is secured via our Foundation Security component, which is included in this service. This set of configurable firewall capabilities manages and controls the traffic passing between the HSCN and the CSP.

This is a network connectivity service. You are responsible for contracting with the CSP(s) directly to obtain their cloud services. This includes any charges that might be incurred.



Ecosystem View

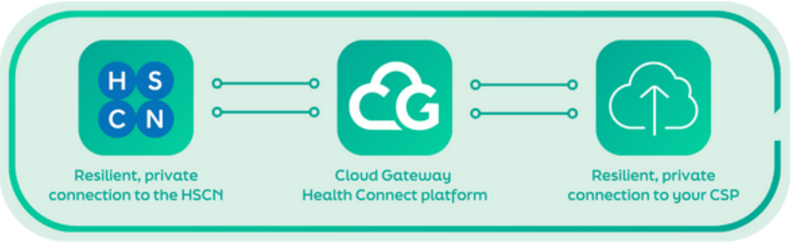

H S C N
Resilient, private connection to the HSCN
Cloud Gateway Health Connect platform
Resilient, private connection to your CSP

Diagram View

Basic operation

Private connectivity to cloud (on-ramp)

To connect to your cloud environment privately, we use a dedicated on-ramp within our data centre presence. This on-ramp gives us access to an aggregated fabric of CSPs.

Each cloud provider has a different method to establish network connectivity. As part of the service, we will engage with you to provide technical guidance during the setup process.

IPSec VPN to cloud

IPSec VPN and routing configuration

We will create 2 x IPSec VPN tunnels to your cloud of choice (for resilience/failover), using the internet as transit. You can terminate the VPN in your cloud using the native VPN Gateway constructs (varies per cloud provider) or using a virtual firewall/router in your virtual network that supports IPSec VPN.

We will then configure BGP (Border Gateway Protocol) or VTI (Virtual Tunnel Interface) type tunnels rather than static crypto-maps - also known as policy-based VPN.

BGP / VTI routing

In order to control traffic paths and allow for dynamic failover should there be any Priority 1 service affecting issues at any point during live service, BGP will be configured across the VPN tunnels. BGP configuration parameters will dictate a primary route to our Point of Presence (PoP) for all traffic, with a secondary PoP as a backup for failover.

BGP AS-PATH prepend will be the main traffic path manipulation technique.

ODS Code and Connection Agreement

All organisations that require access into the HSCN network are required to complete a set of policy documents making up the HSCN Connection Agreement. This must be completed before HSCN Connectivity can be provisioned.

Further information can be found here.

Connecting to the HSCN

HSCN Connectivity provides an IP connection to the HSCN network in line with the HSCN Compliance Framework.

This service can support traffic from your network to the HSCN (outbound, for consuming services), and/or traffic from the HSCN to your estate (inbound, for publishing services). The permitted direction(s) will be defined during onboarding and governed by your use case and firewall policy. If in doubt, please speak to your Cloud Gateway representative to ensure alignment with HSCN policy requirements.

IP Addressing

Details of IP addressing schemes for HSCN Connectivity are defined below:

- You request an IP range (RFC1918) from NHS Digital or you may already have RFC1918 allocated by NHS Digital
- We can use your RIPE range to advertise into HSCN (publically unique address from RIPE)
- We can provide IP maximum of 1 (used for NAT into HSCN)

Note: where public RIPE addressing is allocated for use on HSCN, that address range must not be reachable via the public internet. The address block must not be dual allocated for use on both the public internet and the HSCN network.

Foundation Security

Layer 3 / Layer 4 firewall monitors and controls incoming and outgoing network traffic, based on predetermined security rules. It is designed to establish a barrier between your connected endpoints, whether internal or external traffic.

The below information is required in order to configure firewall policies to allow specific traffic through the platform:

- **Rule Name** - *for example 'ACME RULE'*
- **Source (IP address)** - *for example '1.2.3.4/32'*
- **Destination (IP address)** - *for example '1.1.1.1/32'*
- **Service (Protocol/Port)** - *for example 'TCP/443'*

Acceptance testing

Acceptance criteria

The acceptance criteria for Cloud to HSCN, as part of the platform onboarding are:

- Basic connectivity testing from your CSP to HSCN endpoint(s)
- Failover test between Primary and Secondary connection

Exclusions

The service does not include:

- Internet or MPLS connectivity

Customer responsibilities

You are responsible for:

- Completing and evidencing the HSCN Connection Agreement and ODS Code
- You are not permitted to interconnect endpoints to HSCN via your CSP as this would invalidate our CN-SP obligations towards NHS Digital
- Provision of IP addresses and/or FQDN (Fully Qualified Domain Name) of HSCN services that you require access to
- Requesting an IP address from NHS Digital if using more than one IP
- Setting up and preparing the cloud environment(s) to which the service is connecting
- Providing us with the name of the CSP(s) with which you wish to connect
- Following any instructions provided by us, or the CSP to establish network connectivity. Some steps in the setup process will rely on you, including (but not limited to) acceptance of invitations, and supplying service keys
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- All negotiation, contracts and costs relating to your CSP, including (but not limited to) ingress and egress charges, application running costs and data storage costs
- Ensuring there is no overlapping IP addressing between any networks connecting to the service
- Providing Rule Name, Source (IP), Destination (IP) and Service (Protocol/Port) for each firewall rule that is to be applied
- Ongoing maintenance, management and/or decommissioning of your other security capabilities
- Backups. You are responsible for backing up your own systems. We don't hold customer data. We will back up our own platform, and will store logs as detailed in the Log Storage section below

Cloud Gateway responsibilities

We are responsible for:

- Ensuring our HSCN IP Connectivity is Resilient and ready for you to connect to
- Ensuring you've completed the HSCN Connection agreement prior to live service commencing
- All IP routing including failover and dynamic routing
- Application and management of firewall rules gathered during onboarding process
- 24/7 proactive monitoring of the service
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use)

Ordering and lead time

Ordering and volume

We calculate your cost on a bandwidth basis. The bandwidths available to purchase are:

- 10Mbps
- 25Mbps
- 50Mbps

You can request an increase in bandwidth volume from our Sales Team, or via the Cloud Gateway Portal. During the service contract term, you will not be able to reduce the bandwidth volume.

A standard service request charge applies to HSCN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any HSCN services.

Lead time

Our Service Level Agreement (SLA) to deliver the service is 5 working days. The lead time is measured from receipt of a valid Purchase Order (PO) and contract acceptance, to live service ready for any acceptance testing. The SLA timer will be paused when there is a dependency on you to provide information or input.

Service management

Service support

We have an experienced Service Desk team who are responsible for the day-to-day operational service between you and us.

The Service Desk team's primary responsibility is to provide a single point of contact within Cloud Gateway – to which issues surrounding satisfaction of service may be escalated and resolved.

Support escalations

We strive to ensure that all incidents, service requests, or simple advice and guidance requests from our customers are fulfilled efficiently and effectively within our published timescales.

If you feel that a request is not being managed effectively or would like to escalate a particular issue, this can be raised with our Service Management team.

Complaints

We take complaints seriously and ask that any customer wishing to raise a formal complaint does so in writing to service@cloudgateway.co.uk.

Full details of our complaints procedure can be found within the Cloud Gateway Customer Service Pack, which you will receive during the onboarding process.

Reporting

Various types of reports can be provided. You can request these by contacting service@cloudgateway.co.uk, or raising a ticket via the Cloud Gateway Portal. Charges may apply.

Service levels

The service levels that apply to this service are available in our Service level Agreement (SLA).

Data processing

The data processing terms that apply to this service are available in the Cloud Gateway MSA, found here: https://www.cloudgateway.co.uk/compliance/msa/.

Security arrangements

- The core platform infrastructure that supports this component service is hosted in geographically diverse UK data centres. All data remains within UK sovereignty (with exception if endpoints connect to our platform via the internet)
- We are ISO 27001 and ISO 9001 accredited. We are also compliant with CyberEssentials Plus

Log storage

- All traffic logs and policy controlled events are stored in our Log Aggregation Platform (LAP)
- Logs are retained for 62 days as standard, and are used to populate graphs and visualisations in the Cloud Gateway Portal

Business continuity and disaster recovery

Cloud Gateway maintains a comprehensive approach to operational resilience, ensuring continuity of service through robust business continuity and disaster recovery planning. Our internal continuity and disaster recovery plans are reviewed and tested regularly, and staff receive training to ensure they can respond effectively to a disruption.

Our infrastructure is designed for high availability across data centres. Network component configurations are backed up regularly and can be used to recover from disruptive scenarios. Supplier relationships are governed by rigorous due diligence, including reviews of the supplier's own continuity and recovery practices. Data centres and hosting providers, where under our selection, are selected based on secure practices and continuity capabilities. Certifications held by the supplier are reviewed, such as ISO 22301, ISO 27001, ISO 9001 and ISO 14001.

Our operational model supports full remote working, whereby all staff are equipped to operate securely from the office, home or other locations.

CLOUD
GATEWAY

cloudgateway.co.uk

+44 (0)20 3870 2444

sales@cloudgateway.co.uk

Cloud Gateway
The Ministry, Borough
79 Borough Rd, London SE1 1DN