HSCN Operational Design Overview

Version 5

Published 10 September 2021

Contents

Table of Figures

1 Document Purpose

1.1 Purpose of document

This document provides an overview of the Operational Design for the Health and Social Care Network (HSCN); summarised to enable all stakeholder groups to understand:

- Who is responsible for delivering the different capabilities; and
- How the HSCN operates.

1.2 Scope of this document

This document provides an end-to-end operational description of the HSCN.

1.3 Reader Pre-requisites

The Operational Design Overview should be read in conjunction with the "***HSCN Solution Overview***", which describes the network solution. This document is available on the NHS Digital web page.

2 Executive overview

The stated vision of the Health and Social Care Network (HSCN) Programme was:

"HSCN will enable a future where health and social care unite to transform patient care and services through the provision of greater connectivity, putting data (or) information at the fingertips of clinicians, health and care professionals and citizens".

The spending objectives of the HSCN Programme as detailed in the Full Business Case (FBC) are listed below:

- Support the move from N3 to a new service whilst ensuring future innovation is built in. The first phase of this was completed with the introduction of the Transition Network 1st April 2017.
- Provide integrated connectivity to enable wider health and social care organisations to access national health IT services;
- Deliver a smaller service – that only provides from the centre the infrastructure needed to enable network connectivity across the health and social care system;
- Create a competitive marketplace for interoperable and cost-effective network services;
- A better value for money service – utilise the purchasing power of Government to improve value for money and get the best possible price in part by disaggregating the different parts of the network components to enable a wider variety of suppliers to bid for the work; and
- A shorter contract length that enables more regular market testing to drive down costs.
- Support an Internet First strategy of removing reliance longer term on private networking and providing a migration path to it.

The HSCN programme has established a disaggregated network solution and operating model, based on standards that enable safe and reliable interoperability, a more open marketplace and increased local empowerment.

The programme worked with industry to maintain and grow the established standard-based marketplace of HSCN-compliant Consumer Network Service Providers (CN-SPs) who provide HSCN services directly to consumers.

In addition, the investment for HSCN comprised the following central capabilities:

- **Programme Management** functions, delivered by NHS Digital;
- A **Peering Exchange Network**, which connects HSCN Consumer Networks with each other;
- The **NHS Secure Boundary Service**, formerly known as **Advanced Network Monitoring**, which improves the security of the environment by monitoring and filtering internet traffic on HSCN; and
- **HSCN Authority** functions, delivered or procured by NHS Digital, to manage the operation of HSCN, for example service and security management functions.

The Operational Design Overview describes the business capabilities and interactions for HSCN.

2.1 Document content

Section 3 describes the business capabilities below:

- HSCN Consumers.

- Network Service Providers.
- Secure Boundary Service
- HSCN Authority.

Sections 4 & 5 describe the commercial and operational viewpoints describing the interactions between the capabilities:

- Governance Regime.
- Commercial Model.
- Marketplace.
- In-life Operations.
- Cyber Security.
- HSCN Technology Services.
- Reporting.

3 HSCN Capabilities

This section describes the capabilities involved with HSCN, as shown below.

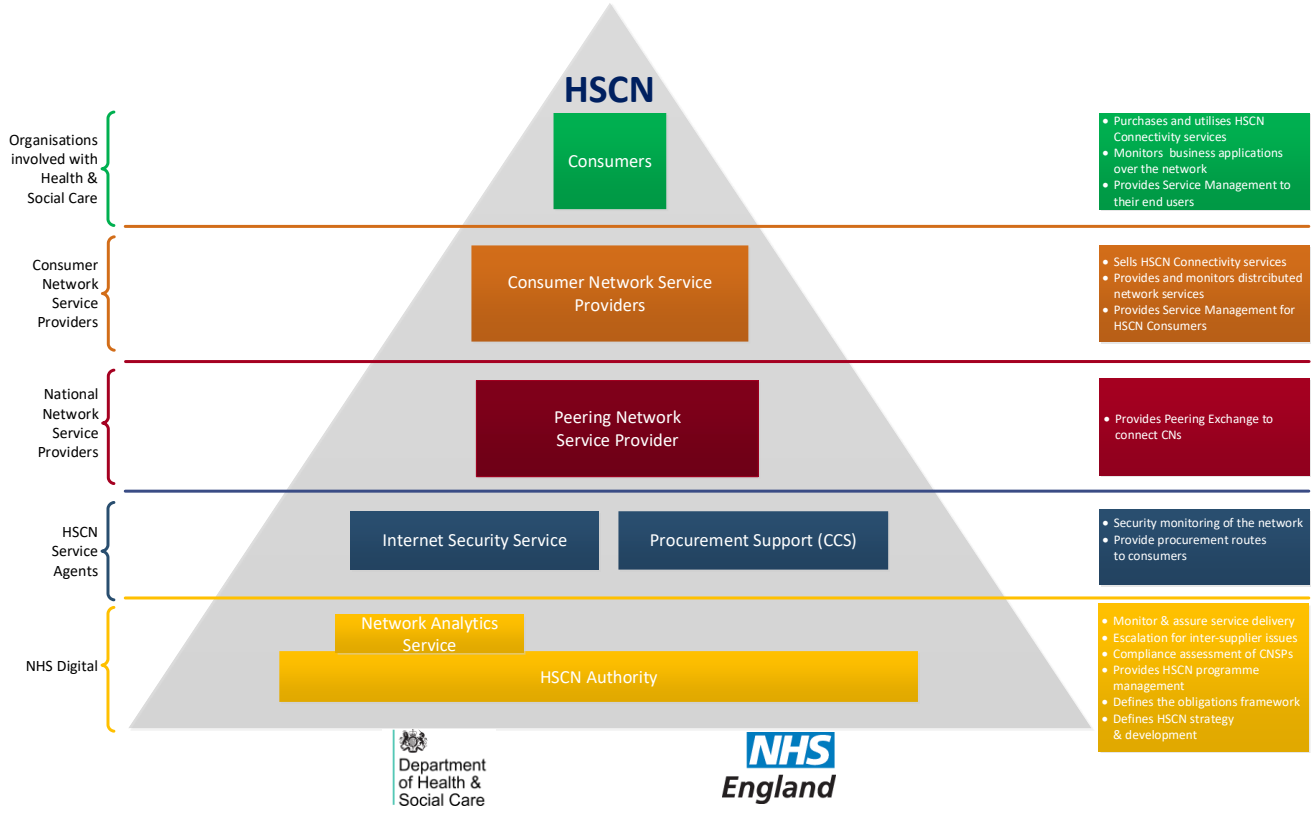

Figure 1: HSCN Capabilities

3.1 HSCN Consumers

The network is used by all organisations that deliver and support Health and Social Care services in England.

HSCN Consumers include all organisations which are connected to the HSCN network and have a valid HSCN Connection Agreement.

The objectives for HSCN Consumers are to:

- Have access to a solution that meets their access and network needs.
- Be offered the right services, at the right price via mechanisms that are easy to use and suitable to their needs.
- Be able to exercise choice in the selection of network services, with respect to both the type of services and between potential suppliers.
- Be able to purchase additional services, outside the scope of HSCN, to complement and/or extend their HSCN network services.
- Receive seamless operation of network services, irrespective of whether the network is being provided by multiple service providers.

3.1.1 HSCN Consumer Organisations

HSCN Consumers fall broadly into three categories:

- NHS organisations (note these are organisations that deliver care in England only);
- Non-NHS Heath and Social Care Organisations; and
- Third Party Support Organisations.

The scope excludes providing funded network connectivity to Scotland, Northern Ireland, Wales, and the Isle of Man. Note that organisations outside of England's borders may purchase HSCN services if required to support business processes.

Each organisation that is permitted to connect to HSCN does this via HSCN Access Connectivity services from CN-SPs. HSCN does not include local network provision or end user devices, and as such HSCN consumers are organisation based.

HSCN Consumers are responsible for paying for and managing the contract with the CN-SP that connects them to HSCN.

NHS Organisations

The following examples are types of NHS organisations that will require HSCN connectivity;

- Clinical Commissioning Groups (CCGs).
- GPs.
- NHS Trusts including:
    - Acute Trusts;
    - Mental Health Trusts;
    - Ambulance Trusts; and
    - Community Trusts.

Non-NHS Heath and Social Care Organisations

In addition, there are a wide range of allied professions and organisations that are permitted to connect to HSCN.

These include the following:

- The wide range of allied professions (i.e. pharmacy, dentistry, and opticians);
- Social enterprise or private organisations such as treatment centres which deliver NHS care under commissioned contracts;
- Any Qualified Provider (AQP) which meet NHS standards and offer best value locally and is commissioned to provide services;
- Local government which plays a key role in health promotion and delivery of adult and social care;
- Central government departments (e.g. MoD, MoJ);
- Prisons; and
- Charity and independent sector organisations.

Note some of these organisations may be funded to access HSCN via other services (e.g. the Electronic Prescription Service providing funding for Pharmacies).

Third Party Support Organisations

There are also a wide range of suppliers of services into the NHS that require network connectivity in order to fulfil their obligations to their customers. These include:

- ICT service providers who require connectivity to support and maintain applications;
- ICT service providers delivering Business Application Services as detailed in the Solution Overview document. These service providers require data centres connected to HSCN such that HSCN end users may consume their applications.

3.1.2 HSCN Consumer Personas

Whilst connections to HSCN are made at organisation level, individuals within that organisation interact directly or indirectly with HSCN.

3.1.2.1 Non-technical Purchaser

This individual is responsible for selecting the optimum service for their End User Organisation. They understand their organisation but have limited technical knowledge and limited time/interest in expanding their expertise. Typically, their organisation will need a simple, relatively low volume connection to the network.

They interact with the HSCN marketplace to procure services.

Their needs are to:

- Buy the right services, at the right price.
- Access advice to inform their choice of appropriate network services.
- Use a purchase mechanism that is quick & easy to use and suitable to their needs.
- Be able to exercise or delegate choice.
- Be able to purchase additional services, outside the scope of HSCN, to complement and/or extend their HSCN network services.
- If they are eligible, benefit from any available central funding when purchasing network services.
- Be able to purchase services to assist in defining the characteristics & design of their network.
- Receive seamless operation of network services, irrespective of whether the network is being provided by multiple service providers.

3.1.2.2 Technical Purchaser

This individual is responsible for understanding the requirements for their End User Organisation and selecting the optimum service. They have technical knowledge relevant to their organisation’s needs. Their network requirements will range from simple connections from an individual site to more complex designs with multiple connections between sites and to the HSCN network.

They interact with the HSCN marketplace during the design and purchase of services.

Their needs are to:

- Have access to a solution that meets their access and network needs.
- Be offered the right services, at the right price via a mechanism that is easy to use and suitable to their needs.
- Be able to exercise choice in the selection of network services, with respect to both the type of services and between potential suppliers.
- Be able to purchase additional services, outside the scope of HSCN, to complement and/or extend their HSCN network services.
- Be able to purchase services to assist in defining the characteristics & design of their network.
- If they are eligible, benefit from any available central funding when purchasing network services.
- Receive seamless operation of network services, irrespective of whether the network is being provided by multiple service providers.

3.1.2.3 Network Manager

This individual is responsible for supporting the End User Organisation's network and for engaging with supplier and service organisations.

Irrespective of the sourcing route used for the procurement, they will interact with their service provider to report & resolve issues.

Their needs are to:

- Receive seamless operation of network services, irrespective of whether the network is being provided by multiple service providers.
- Be able to report issues to single point for resolution, irrespective of whether the network is being provided by multiple service providers.

3.1.2.4 End User

This individual accesses applications and data that are only accessible with an HSCN connection. These users access these from their local network via their organisation's connection to HSCN. Specific features of interest to End Users, such as remote or mobile access, operate over the HSCN network but are outside the remit of HSCN delivery.

They will not interact directly with any HSCN capability but will be represented by their organisation's purchaser and network manager for purchasing and issue resolution activities respectively.

Their needs are to:

- Have access to National Applications and data that are only available using a connection to HSCN.
- Receive seamless operation of network services, irrespective of whether the network is being provided by multiple service providers – including the provider of their local network.

3.1.3 HSCN Connection Agreement

HSCN uses a Connection Agreement (CA) for end organisations that covers business need, basic cyber security best practice and key contact details (including cyber security contacts).

The HSCN CA requires industry standard cyber security hygiene for an organisation before it can connect. This serves both as an education activity (that the organisation has to plan for cyber security) and improves the security hygiene of the wider ecosystem. This has replaced the Information Governance Statement of Compliance (IG SoC) that was required for N3 connectivity and serves more as a security support function, than requiring an organisation to meet stringent local security controls and procedures. Note that this assessment is undertaken by the HSCN Authority.

The CA is intended to be a control of who is connected to the HSCN – is the organisation eligible to connect; is a specific consumer model of connection required; type of organisation connecting is permitted.

3.2 Network Service Providers

HSCN will employ Consumer Network Service Providers (CN-SPs) to provide specific elements of the network, as shown below.

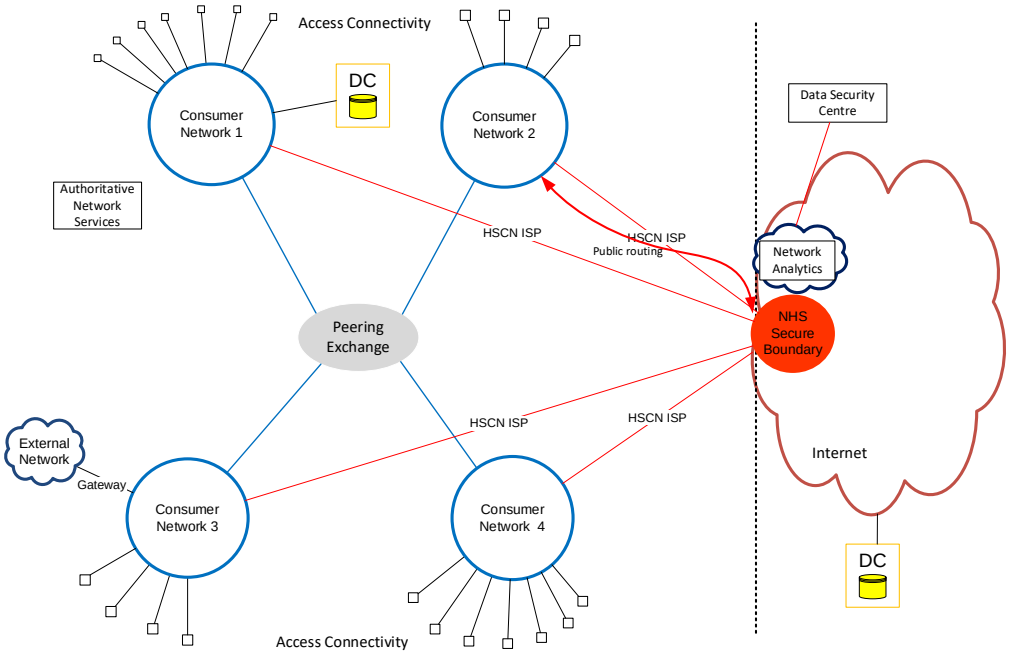

Figure 2: HSCN Network Architecture

Consumer Network Service Providers (CN-SPs) supply the HSCN Components as documented in the HSCN Solution Overview.

The objectives for CN-SPs are (where applicable) to:

- Ensure that HSCN Consumers experience seamless operation of network services, working with the HSCN Authority Service Coordinator function and other CN-SPs;
- Understand and offer services that align with HSCN strategy objectives for disaggregated services; and

- Choose appropriate routes to market for their services.

The CN-SPs also provide the required service management wrap for the delivery of their services governed under the HSCN Authority Service Coordinator function. To do this the CN-SPs are required to work to the Service Management Approach as detailed in Section 4.

3.2.1 Consumer Network Service Providers (CN-SPs)

HSCN CN-SPs operate by providing access and distribution services locally to HSCN Consumers by doing the following:

- Provide HSCN Access Connectivity as a range of blended services providing varied bandwidth requirements, availability, and resilience options to individual sites (e.g. NHS Hospitals, Primary Care, Community & Mental Health, CCG, Care Homes, 3rd Parties etc.).
- Connection to the Peering Exchange Network supporting required HSCN traffic flows.
- Route internet traffic to the NHS Secure Boundary Service
- Routing options to a group of connected HSCN Consumers for closed user group routing delivered by the CN-SPs network.
- HSCN Consumer service provision for maintaining a Consumer's HSCN service.

The CN-SPs are the direct suppliers to the HSCN Consumer base for provisioning and service management.

CN-SPs are approved to deliver HSCN Services under the HSCN Compliance Process (see Section 4.1). CN-SPs need to demonstrate via this process that they meet the HSCN Obligations to provide the required connectivity for HSCN Consumers to share data, and interoperate with other parties including the HSCN Authority, Secure Boundary Service, and other CN-SPs.

It is the responsibility of the CN-SP to provide a Service Desk to their HSCN Consumers, and work to the HSCN Service Model for incident control across the HSCN components with other providers. The CN-SP is responsible for owning the HSCN Consumer interface until incidents are resolved.

CN-SPs offer services to HSCN Consumers which include the technical functions to be delivered and the service regime including service levels and responsibilities. HSCN Consumers order services direct from CN-SPs who are responsible for order receipt, management, and billing.

3.2.2 Peering Network Service Provider (PN-SP)

The HSCN Authority contracts directly with the Peering Network Service Provider (PN-SP). The PN-SP supplies a peering service to which all CN-SPs are connected. CN-SPs route traffic between each other through the peering network. The peering network is based at two carrier neutral hosting locations which are geographically separated (London and Manchester). All CN-SPs have connections to both locations. The Peering Exchange is currently provided by Redcentric.

The Peering Network Service Provider provides an incident management service desk to directly connected CN-SPs. The Peering Network Service Provider works with the HSCN Authority Service Co-ordinator function to ensure that cross supplier incidents are managed to resolution. It does not provide direct connectivity services to HSCN Consumers.

3.3 NHS Secure Boundary Service

HSCN CN-SPs direct all internet bound traffic towards the NHS Secure Boundary Service. Outbound and returning inbound Internet traffic is subjected to the Secure Boundary Service processes. The Secure Boundary Service is a cloud service provided by a Secure Boundary Service Agent directly contracted by the HSCN Authority.

The Secure Boundary Service includes processes to block known malicious activity to, and returning from, the internet.

The Secure Boundary Service provides logging and reporting functions; with events and reports which are specified by the HSCN Authority.

More information on Secure Boundary can be found here.

3.4 HSCN Authority

The HSCN Authority ('Authority') is the delivery function that ensures that the HSCN meets its overall objectives and will be the owner of the overall business change. NHS Digital fulfils this function on behalf of the Department of Health and Social Care (DHSC), the sponsor of the HSCN.

The Authority:

- Oversees all HSCN operational matters;
- Enables more direct control over the HSCN supplier ecosystem; and

.

The HSCN Operating Model consists of several functions:

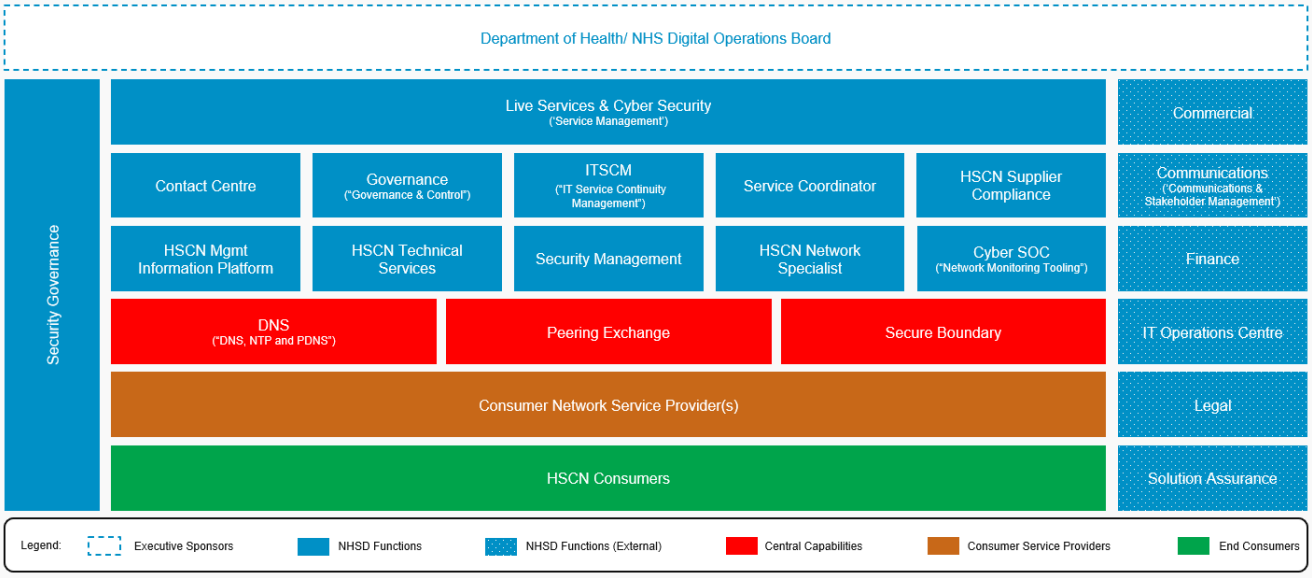

Figure 3: HSCN Operating Model

A summary of key HSCN Authority functions is provided below:

Function	Summary
Strategy	• Strategic direction for further HSCN enhancements and transformation, including Internet First (through NHS Digital's Network and Connectivity Programme)
Finance	The 'Finance' function provides accounting and financial reporting for HSCN. Responsibilities include: • Provide programme financial investment reporting to the DHSC demonstrating value for money.
Benefits Reporting & Realisation	The 'Benefits' function operated as part of the HSCN Programme and provided benefits reporting and promoted the realisation of benefits by NHS Trusts through the life of the Programme. Responsibilities included: • Provide benefits reporting to the DHSC demonstrating achievements of targets. • Work with HSCN Consumers to realise and report benefits.
Commercial & Procurement	The 'Commercial' function provides commercial management and assurance of contracted Suppliers and provides commercial and procurement expertise to support HSCN. Responsibilities include: • Maintain relationships with directly engaged HSCN Service Providers and HSCN Service Agents. • Manage an effective relationship with Crown Commercial Service to provide Procurement Support expertise into HSCN. • Liaise with CCS, suppliers, and consumers to ensure that the HSCN offerings are relevant and straightforward to purchase. • Assure the contracting model so that it is effective within the disaggregated supply chain. • Recognise and implement opportunities for further synergies between the parties as the relationship matures. • Ensure that the marketplace and supporting services continue to operate in line with HSCN objectives.
Governance & Control	The 'Governance' function provides oversight of the Authority functions, strategic direction for HSCN and future enhancements (including initiating new projects). Responsibilities include: • Providing effective governance across service delivery and the HSCN supply chain. • Ensuring alignment of HSCN Objectives to programme delivery and other IT Strategies. • Ensuring HSCN is managed effectively by NHS Digital on behalf of the DHSC. • Act as the highest level 'ombudsman' type-role for conflict resolution on behalf of the service.
Communications & Stakeholder Management	The 'Communications' function will manage engagement and communication with parties involved in HSCN including Suppliers and Consumers. Responsibilities include: • Ensure effective communication between the Authority, CN-SPs and HSCN Consumers. • Maintain the HSCN Website.
Architecture	The 'Architecture' function provides technical assurance of the solution, technical expertise to support HSCN and collaboration with other NHS Digital and Government initiatives. Responsibilities include:

Function	Summary
	• Articulate HSCN Consumer requirements into technical, service and security requirements for the development and continuous improvement of HSCN services. • Maintaining HSCN Obligations Framework including technical and service management standards and policies. • Maintaining the HSCN Technology Roadmap. • Supplier engagement on future services and technical developments • Consistent communication and application of HSCN network principles across HSCN and HSCN consumers as a single point of operation for all network architecture concerns.
Security Governance	The 'Security Governance' function provides security assurance of the solution, specialist expertise to support HSCN and guidance to Suppliers and Consumers. Responsibilities include: • Consistent communication and application of security principles across HSCN and serves as a single point of operation for all security-related activities. • Delivering Network Analytics Service to work with the Data Security Centre team.
Security Management	The 'Security Management' function will provide management of security events and incidents during day-to-day operations. Responsibilities include: • Effectively managing security threats and incident across HSCN.
Service Management	The 'Service Management' function will provide ITIL aligned management of centrally contracted service providers (including Peering Network Service Provider and Secure Boundary Service Provider) on day-to-day operations. Responsibilities include: • Provide management and coordination for HSCN Service Agent and National Network Service Provider services. • Acting as the Service Co-ordinator, provides oversight over the Consumer Network Service Providers
Service Co-ordinator	The 'Service Co-ordinator' function will provide operational oversight and performance management of CN-SPs, acting as an escalation point for operational issues involving CN-SPs.
Technical Services	The 'Technical Services' function consists of components that underpin the HSCN. Responsibilities include: • Domain Name Service (DNS) administration – allocating/managing DNS entries. • Providing IP Address Management (IPAM) to co-ordinate allocation of IP addresses to consumer services across HSCN. Note that all Network Service Providers manage set-up and use of IP addresses on their services and include their own IP address management functions. • Performing support for the investigation of incidents and problems. • Network Time Protocol (NTP) - Management of an interim Network Time Protocol (NTP) service for HSCN Consumers, provided by the DNS Supplier (Accenture). AWS accounts owned and managed by NHS Digital Live Services
Network Analytics Service (NAS)	The Network Analytics Service (NAS) will supplement the Data Security Centre service by ingesting network telemetry data in near real time and performing proactive and reactive analysis on the data in order to identify any malicious activity taking place over HSCN. The NAS will identify the organisational source of any malicious activity in order that corrective action can take place.

Function	Summary
HSCN Supplier Engagement	The 'Supplier Engagement' function will manage non-operational engagement with CN-SPs and act as custodian of the Supplier Compliance Regime. Responsibilities include: • Managing and maintaining the HCSN compliance regime and Obligations Framework. • Provide support to CN-SPs through the compliance assessment process. • Monitor compliance and respond to CN-SP breaches of the Obligations Framework. • Issue and rescind or terminate Compliance for CN-SPs.
HSCN Consumer Support	The 'Consumer Support' function will manage engagement with End Customers and act as a custodian for the HSCN Management System and Connection Agreement. Responsibilities include: • Managing and maintaining HSCN Consumer Connection Agreement requests. • Providing support to HSCN Consumers during deployment and in-life operations • Proactively supporting Health and Social Care communities of interest and regional partnerships to design future solutions.

3.4.1 HSCN Programme

The transition and transformation to the HSCN service was managed by the HSCN Programme which was responsible for:

- Defining and implementing HSCN Service Agent and National Network Service Provider services and putting in place commercial contracts for these.
- Establishing the HSCN Authority.
- Assurance of the delivered service.
- Overseeing the migration from the Transition Network services. This process is now complete.
- Co-ordinating and driving the migration of Consumers to HSCN (including support in procuring HSCN services). This process is now complete.

The HSCN Programme have completed all migrations and related actions. The programme was shut down and solution handed over the Service Management in December 2020.

3.4.2 Service Management

3.4.2.1 NHS Digital Service Management

The NHS Digital Service Management function provides service management of the Peering Network Service Provider and the Secure Boundary Service Provider.

They are responsible for providing standard service management processes and functions.

3.4.2.2 Service Co-ordinator

- The Service Co-ordinator function resides within the NHS Digital Live Services function and provides operational oversight of all CN-SPs within the disaggregated HSCN model. Performs performance monitoring of CN-SPs and acts as a facilitation and escalation point between CN-SPs and NHS capabilities (where appropriate) to coordinate issue resolution.

The Service Coordinator function provides the following services (described below):

- Provide a service management interface for CN-SPs and HSCN Central Capabilities;

- Act as an incident management escalation point for CN-SPs and HSCN Central Capabilities;
- Coordinate Multi-Supplier Interventions involving CN-SPs, Central Capabilities and where required HSCN consumers;
- Provide problem management governance of CN-SPs;
- Provide change management governance and integration with CN-SPs and all other HSCN service providers
- Act as a capacity management escalation point for CN-SPs;
- Participate in continuous service improvement;
- Monitor performance of CN-SPs;
- Oversee service improvement activities for CN-SPs;
- Monitor maintenance of CN-SP data;
- Manage CNSP/CCS complaints;
- Support Supplier Compliance (as 'Service Management Specialist'); and
- Manage HSCN Consumer access restrictions.

Provide a service management interface for CN-SPs – Act as an interface between NHS Digital service management teams (including Incident, Problem, Change and Capacity management) and CN-SPs in the first instance. Activities include:

- Provide a single point of contact for NSPs and Functions.
- Respond to escalations from CN-SPs, CCSPs or other functions, initiating the appropriate response as described below.

Perform Incident Management – Provide integrated incident management across HSCN including:

- Monitor the investigation and resolution of HSSI's impacting HSCN.
- If required, intervene with the management and investigation of HSSIs.
- Engage other NHS Digital service management teams and/or suppliers to support the diagnosis, investigation and resolution of issues where the root cause is unknown.
- Acting as the Service Coordinator, initiate Multi-Supplier Interventions to engage with CN-SPs to help support the investigation, diagnosis and resolution of incidents impacting HSCN.
- Receive updated contact details for key staff from CN-SP and oversee updates to internal records.
- Inform CN-SPs of potential network issues that are identified by or reported to the Service Coordinator (directly or via NHS Digital Service Bridge).
- Provide a service management escalation point for HSSIs involving CN-SPs.
- Receive reports of new and updates for existing HSSIs from CN-SPs.
- Receive HSSI dataset(s) and log a corresponding incident within NHS Digital Cherwell tool.
- Update the NHS Digital Communications Tool and Service Status Page with details of HSCN HSSI(s) affecting Central Capabilities or other National Services.
- Initiate and co-ordinate Multi-Supplier Incidents involving CN-SPs where requested by a NSP, CN-SP or Function (as described below).
- Receive and review CN-SP HSSI reports to ensure appropriate actions have been taken to resolve incidents and prevent their reoccurrence.
- Formally accept or reject HSSI reports, providing feedback when they are not accepted and direct corrective action.

- Monitor and record poor supplier performance engaging, investigating and supporting resolution of incidents (as described below).
- Escalate to a CN-SP senior management to ensure an adequate response.
- Triage with the NHS Digital Clinical Safety Team for any HSSI's which impact clinical safety.
- If required, access CN-SP Dashboards to view monitoring tooling and independently verify the status of network activity.
- Perform trend analysis and reporting of CN-SP HSSI's to inform performance management, problem management and service improvement activities.

Coordinate Multi-Supplier Incidents involving CN-SPs – Where requested by a NSP, CN-SP or Function, initiate a Multi-Supplier Intervention (MSI) (subject to validation) including:

- Record HSSIs and any subsequent updates with NHS Digital Cherwell that are reported by NSPs.
- Direct and co-ordinate investigation activities through to resolution, engaging with affected CN-SPs as required and convene MSI service bridges where required.
- Provide updates on MSI HSSIs to HSCN senior management.
- Escalate to a NSPs senior management where an NSP is providing an inadequate response or is failing to meet its HSCN Obligations.
- Monitor and record poor supplier performance (as described below).

Perform Problem Management – Provide problem management governance across HSCN including:

- On a monthly basis, review significant degradation problem updates reported by each CN-SP to ensure sufficient progress is being made and identify trends.
- Receive and review CN-SP problem management reports (received monthly) to validate appropriate actions have been taken.

Perform Change Management – Provide integrated Change management and governance across HSCN including:

- Receive FSCs provided by CCSPs and CN-SPs and produce an HSCN RAMP.
- Facilitate and chair the HSCN Change Advisory Board as required.
- Communicate planned changes within NHSD.
- Notify CCSPs of upcoming major changes by distributing the NHS Digital RAMP.
- Acting as the Service Coordinator, manage any change clashes to resolution between CN-SPs and other suppliers.
- Provide visibility of change across HSCN by maintaining the NHS Digital Forward Schedule of Change (FSC aka NHS Digital RAMP).
- Ensure that the NHS Digital FSC is made available to CN-SPs to inform planning.
- Collate details of change activity provided by CN-SPs via weekly FSC submissions.
- Provide collated FSC to NSPs and the HSCN Change Advisory Board.
- Carry-out clash management where necessary, working with NSPs to reschedule changes that may adversely impact each other.
- Receive and record details of HSCN Consumer impacting emergency changes from CN-SPs.
- Facilitate the assessment of major HSCN changes initiated by the HSCN Authority or an NSP including:
- Identify and issue impact assessment requests to CN-SPs affected by planned changes.

- Receive RFCs from CN-SPs and facilitate their assessment and response to CN-SPs.

Participate in continuous service improvement – Participate in continuous service improvement activities engaging with CN-SPs (as described under Service Management) including:

- Chair and host joint CSI forums.
- Promote innovation with all service providers.

Monitor performance of CN-SPs – Continually monitor CN-SP performance, based upon receipt of CN-SP Performance Reports and other direct feedback, initiating corrective activity where necessary. Activities include:

- Monitor adherence to service management sections of the HSCN Obligations.
- Oversee the submission and receipt of CN-SP performance reports uploaded to the HSCN Management System (provided monthly).
- Identify and escalate failures of CN-SPs to meet the Compliance Obligations Framework. Trigger the process of via the commercial function, triggering service improvement activities where appropriate.
- Manage non-conformance to HSCN Service Management Obligations, escalating through the CRG process if necessary.
- Inform CN-SPs of poor performance and initiate service improvement activities where necessary.

Oversee service improvement activities for CN-SPs – In the event of poor CN-SP performance, initiate service improvement activities including:

- Facilitate and chair Performance Improvement Review Group(s) to initiate Service Performance Reviews with CN-SPs where agreed triggers have occurred and monitor completion.
- Direct CN-SPs to produce a Service Improvement plan where agreed triggers have occurred.
- Monitor and track Service Improvement implementation through to completion (via Performance Improvement Review Groups).
- In the event a CN-SP fails to implement the Service Improvement Plan or continued reports of poor performance from impacted HSCN Consumers are received, escalate through the CRG process as necessary to decide upon further action.

Perform Capacity Management – Act as a point of escalation for CN-SP in relation to capacity management including:

- Facilitate discussions between Suppliers and define actions to remediate capacity issues.
- Support HSCN tracking of key capacity constraints and major ‘system’ changes, communicating to CN-SP/CCSPs as appropriate.

Monitor maintenance of CN-SP data – Oversee supplier updates of company information, contact details and estate data which are required for day-to-day operations including:

- Ensure relevant CN-SP data, including contact details and the HSSI Minimum Dataset is stored and kept up to date.
- Track that suppliers are making available and updating contact details.
- Contact suppliers to investigate and resolve any issues where out-of-date or inaccurate contact details have been provided.

- Engage CN-SPs to resolve any data quality or submission issues.

Manage complaints and escalations – Manage complaints between NSPs with regard to persistent failure to fulfil their incident management responsibilities including:

- Operate a single point of contact and service management escalation for all NSPs.
- Receive complaints raised by NSPs with regard to a persistent failure by another NSP to fulfil their incident management responsibilities.
- Record and monitor a log of captured NSP complaints.
- Initiate service improvement activity with any CN-SP that is a subject of complaint or has failed to meet their service levels and/or HSCN obligations.
- Escalate breach of HSCN obligations to Commercial via the CRG process if required.

Maintain access to CN-SP Dashboards – Retain current and active user access to CN-SP service dashboards to support investigation and diagnosis of incidents including:

- Securely store user access details, test and keep these up to date as per the CN-SP access control standards.
- Undertake any training for user access.

Support Supplier Compliance– Participate in the Compliance Regime as the 'Service Management Specialist' by:

- Assist the assessment of prospective suppliers in their ability to fulfil the service management obligations as directed by work-packages issued by the Compliance Manager (within Supplier Compliance).
- Attend and participate in the Compliance Review Group to:
- Review Supplier applications and provide a recommendation to the Compliance Assessment Board.
- In response to a CN-SP breach of the obligations, convene and agree on appropriate action. Input into changes to the compliance process, to ensure that it is technically fit for purpose and approve any updates (as per the change control process).

3.4.3 The HSCN Website

The HSCN Website hosted on the NHS Digital website provides information and links to the following services.

3.4.3.1 For Consumers

- Overview of what HSCN is and what is provided
- Help and support information to guide HSCN Consumers including:
    - Applying for funding;
    - Connection Agreement process;
    - HSCN services design advice;
    - Procuring HSCN services;
    - Connecting to HSCN services; and
    - Technical guidance, policies, and best practice documents.

- Details on the range of HSCN service offerings, including a list of the suppliers that are HSCN Compliant and offering HSCN services.
- Sign posting to other external sources of information and how to get more detailed support.

3.4.3.2 For Suppliers

- How to become an HSCN Consumer Network Service Provider including applying for HSCN Compliance.
- Information on providing details of HSCN services and how to offer services via the various procurement routes.
- Details of the HSCN Obligations Framework.
- Details of HSCN documents (e.g. The HSCN Deed and Liability flows).

4 Operational viewpoints

This Section describes the operational viewpoints documenting the interactions between the Business Capabilities described in Section 3.

- Compliance Process
  - Obligations Framework
- In-Life Operations:
  - Deployment of services;
  - Service Assurance; and
  - Service Integration and Service Management.
- Cyber Security
- HSCN Technology Services
- Reporting.

4.1 HSCN Compliance Process

4.1.1 Initial Compliance

The HSCN Obligations Framework sets the minimum compliance levels that HSCN CN-SPs must meet and how HSCN Compliance is demonstrated.

The compliance process undertakes an assessment of a particular supplier so that the services they provide are assured to meet the relevant HSCN Obligations. Therefore, note that this compliance is to enable the supplier to become a CN-SP. This is not to assure compliance for a particular HSCN Consumer contracted service.

HSCN Suppliers needs to produce the relevant evidence that they meet the obligations. The process and required evidence is detailed in the HSCN Compliance Operating Model published on the HSCN Website.

The Compliance model is made up of 3 core stages:

- **Stage 1 (Pre-market):** The relevant obligations which must be met before a Supplier can market/sell HSCN-badged services.

- **Stage 2 (Pre-live):** The relevant obligations which must be met before a Supplier can begin supplying services to Consumers.

- **Stage 3 (Post-live):** The relevant obligations which can only be proven by Supplier performance once the Supplier is supplying HSCN services. As part of Stage 3 Compliance, there will be regular assessment of Supplier performance and adherence to the HSCN Obligations Framework.

Through the process, Suppliers need to produce the relevant evidence that they meet the obligations. This could be documentation, design, relevant external compliance, or audit review of operations.

The HSCN Authority makes the final decision as to whether or not the Supplier achieves HSCN Compliance.

In order to achieve Stage 1 HSCN Compliance, the HSCN Authority and the CN-SP are required to sign the CN-SP Deed. The HSCN Authority reserves the right to audit a Supplier at any time based upon report findings and or escalations from other parties.

The HSCN Authority is responsible for managing CN-SPs that breach their obligations in accordance with the procedures set out in the Deed.

4.1.2 HSCN Compliance Renewal

Once a CN-SP has become HSCN Compliant, they are eligible to supply HSCN Services to HSCN Consumers.

There is an annual renewal cycle of HSCN Compliance. The details of this can be found in the HSCN Compliance Operating Model which can be found on the HSCN website.

4.1.3 HSCN Compliance Revocation

Supplier non-performance of services may result in the HSCN Authority putting a stop on a CN-SP's sales or a CN-SP's compliance being "revoked". Suspension will permit the supplier to continue service to existing HSCN Consumers; but prevents further sales until the HSCN Authority is satisfied that the non-performance has been rectified. Revocation suspends future sales and initiates a set of activities to transition all existing HSCN connectivity contracts held by that CN-SP.

4.1.4 HSCN Obligations Framework

HSCN operates in accordance with the HSCN Obligations Framework, which principally covers a set of HSCN Obligations that include adherence to Policies and Standards for:

- Operations and Governance – Behavioural, Commercial;
- Technical and Security – Network controls, monitoring and Security controls; and
- Service – Service management, Testing and Assurance.

HSCN Obligations	• Output based statements but with agreed measurable statements where necessary • A set of HSCN Obligations that encompass how HSCN operates end to end • Details which specific obligations apply to specific providers i.e. not all obligations apply across the board • Are written to include an obligation that Policies and Standards must be met/delivered and that HSCN Guidance is used for implementation details
HSCN Policies	• DHSC/NHS Digital policy on how HSCN interoperates and/or technical policy that affects how the network works • The set of Policies which apply to HSCN set by HSCN Authority • Flexible – can change but will be infrequent and only when major changes are required – would be under change control depending on contract and what is included
HSCN Standards	• Industry agreed standards expected to be adopted by suppliers where appropriate • Enforceable by contract measures, compliance and/or audit

	• Which Standards apply to HSCN set by HSCN Authority • Flexible – can change but will be infrequent and only when major changes are required – would be under change control depending on contract and what is included
HSCN Guidance	• Detailed implementation documentation – the detail behind policies • Written and supplied by all organisations within HSCN operating model • Assured by HSCN Authority • Flexible – can change and will be for HSCN Consumers and their suppliers to instigate change control depending on individual contract • Open document under common licence

For more information on the Obligations, please refer to the CN-SP Obligations Framework, published on the HSCN Website.

4.2 In-life Operations

The HSCN Compliance process specifies the standards needed before a supplier can offer HSCN services. Suppliers are also obliged to work with HSCN in order to deliver integrated, secure services to their HSCN Consumers.

4.2.1 Deployment of services

The approach summarised below is followed for all deployments, irrespective of procurement route:

1. The Consumer procures a service.
2. The Consumer and CN-SP enter into an agreement including the HSCN Mandatory Supplemental Terms:
3. The CN-SP commences technical activities.
4. The Consumer completes a Connection Agreement:
    a. The Connection Agreement is lodged with the HSCN Authority.
    b. The HSCN Authority approves the Connection Agreement.
5. The CN-SP completes technical activities and commences service introduction activities.
6. The CN-SP confirms with the HSCN Authority that the Connection Agreement has been approved.
7. The Service goes live:
    a. The CN-SP informs the HSCN Authority Service Co-ordinator function that the service is live.
    b. The Service Co-ordinator function informs the Data Security Centre team that the service is live.

The NHS Digital HSCN website hosts a number of documents that provide more information.

4.2.2 Service Assurance

The CN-SP has to demonstrate that the network solution provided to the Consumer is correctly configured and allows the appropriate routing to the agreed HSCN end points and supplies the agreed capacity to the HSCN Consumer.

CN-SPs:

Work with the Consumer to produce an agreed test approach, test plan and test scripts.

- The test plan as a minimum should contain the following tests:
  - Send from the Consumer's location an http request to an agreed web page using the CN-SP internet gateway.
  - Send from the Consumer's location an http request to an agreed web page hosted by the CN-SP.
  - Send from the Consumer's location an http request to an agreed web page hosted by NHS Digital and with an HSCN private address.
- Carry out specific Consumer testing as part of the deployment assurance as agreed in the test plan.
- Work with the Consumer and technical stakeholders to resolve test failures.

4.2.3 Service Integration and Service Management

Every Network Service Provider and Service Agent is fully accountable and responsible for the service management and delivery of their own services, using processes and techniques as described in best management practice such as ITIL® or equivalent.

Every CN-SP is required under the HSCN Obligations Framework to work with other NSPs and the HSCN Authority Service Co-ordinator function in delivery of the overall HSCN service. In addition, the CN-SP signs a Deed of Undertaking with the HSCN Authority, which provides the Authority with legal remedies to address critical failures that cannot be addressed by one consumer contract.

CN-SPs are responsible for providing service management processes and functions and day to day interactions with their Consumers as described within the HSCN Obligations Framework (please refer to the service management section and CN-SP Service Management Addendum for further information).

4.2.3.1 Service Management standards

The ISO/IEC 20000 standard for IT service management, ISO 9001 for quality management and the ISO/IEC 22301 standard for business continuity management systems provide an independent assessment of an organisations capability in these areas.

CN-SPs should, at an organisation level, be accredited to ISO 9001 and ISO 27001 as well as ISO/IEC 20000, and ISO/IEC 22301 standards, or should operate in a manner that is equivalent to the requirements of those standards and should apply those standards to the provision of HSCN Services.

4.2.3.2 Service management tooling approach

HSCN does not mandate adoption of particular tools for service management; every Network Service Provider is free to make their own choice.

4.3 Cyber Security

In order to reduce the cyber threat to the HSCN environment, a layered security approach is taken. Each Supplier is responsible for the security of their service to their network boundaries, as required by their contract, the HSCN Obligations Framework and the HSCN Consumer requirements.

The oversight of security of the network is under the remit of the NHS Digital Data Security Centre.

4.3.1 Network Analytics Service

The NHS Digital Data Security Centre incorporates a Network Analytics Service (NAS) to understand cyber threats to HSCN and the wider Health and Social care system.

The NAS supports these functions by:

- Centralised collection of network “telemetry” data from the environment.
- Filtering, storage, and automated processing of the “telemetry” data to identify potentially malicious traffic.
- Investigation of identified traffic to validate if it is malicious, and which organisation(s) is (are) affected by it.
- Reporting of the incident to the appropriate organisation, and support issue resolution.
- Creation and maintenance of a “playbook” that details scenarios that may occur (or have occurred), and the course of action to resolve the incident.
- Provision of a subset of telemetry data to the NHS Digital service integration toolset for the monitoring of overall network health.
- Work with other HSCN capabilities such as NHS Secure Boundary and the HSCN Authority Service Co-ordinator function.

To support the collection of the telemetry data CN-SP’s are responsible for providing the following data sets upon the commencement of the HSCN service:

- The capture of IPFix data from the Customer Premise Equipment that is used by HSCN Consumer organisations to access HSCN network services.
- Delivery of IPFix data to the NAS.
- Maintain an asset register of HSCN infrastructure used to deliver HSCN network services.

For a description of monitoring locations and data flows please see the HSCN Solution Overview.

The HSCN Authority has the ability to control access to HSCN services through access control lists that CN-SPs are expected to implement.

- Ability to centrally deploy Access Control Lists that map to all Customer Premises Equipment as directed by the NHS Digital Data Security Centre team.
- Ability to deploy customised Access Control Lists that map to an individual Customer Premises Equipment as directed by the NHS Digital Data Security Centre team.
- Organisations wishing to be connected to HSCN must agree to a Connection Agreement which will document the policies and procedures they must follow to be allowed to use HSCN services.

4.3.2 NHS Secure Boundary

HSCN CN-SPs direct all Internet bound traffic towards the NHS Secure Boundary Security Service. Outbound HTTP Internet traffic is subjected to NHS Secure Boundary Service processes. The NHS Secure Boundary Service is a cloud service provided by a NHS Secure Boundary Service Agent directly contracted by the HSCN Authority.

The NHS Secure Boundary Service includes services to block known malicious activity as follows:

- Malware;
- Zero-day malware;
- Worms;
- Virus;
- IP Addresses and URLs;
- botnet traffic;
- Command and control communications; and
- Attempts or potential attempts to infiltrate data.

The NHS Secure Boundary Service provides logging and reporting functions; with events and reports specified by the HSCN Authority.

4.3.3 Protective DNS

HSCN DNS traffic is directed to the National Cyber Security Centre Protective DNS (PDNS) service. PDNS prevents access to domains known to be malicious by simply not resolving them. This prevents access to malware, ransomware, phishing attacks, viruses, malicious sites, and spyware at source.

4.4 HSCN Technology Services

In order for HSCN to be a multiple supplier network, while as the same time providing a consistent delivery of service, NHS Digital supplies two capabilities:

4.4.1 DNS

- Administration of DNS change requests from the HSCN Authority in accordance with HSCN DNS Policy in association with specific SLAs.
- Provides high availability Authoritative DNS services.
- Operates a domain name registry for the nhs.uk domain, registering domain names on behalf of the NHS and the HSCN Authority in accordance with the NHS Domain Name Policy and relevant industry internet standards.
- The domain name registry contains a list on a Customer by Customer basis of all registered nhs.uk domain names.

4.4.2 IP Address Management

- Allocates IP addresses for use on the HSCN and manages a registry of IP addresses for customers connected to the HSCN in compliance with the NHS IP Addressing Policy.

- Co-ordinates the HSCN Authority IPAM function, the allocation of IP addresses, and the return of unused IP addresses.

4.4.3 NTP

- NTP is a networking protocol for clock synchronisation between computer systems over packet-switched, variable-latency data networks.
- Whilst the interim Network Time Protocol (NTP) service for HSCN Consumers is currently provided by the DNS Supplier, AWS accounts are owned and managed by NHS Digital Live Services, and NHS Digital requires all organisations to reconfigure their time sources from the NTP service to a set of new sources and must carry out their own risk assessment to determine clinical and operational requirements for their NTP solution.

4.5 Reporting

NSPs and Service Agents provide normal financial and service level reporting to the HSCN Authority as per the agreed contracts.

CN-SPs provide reporting to their Consumers as per their respective contracts and shall also provide additional reporting to the HSCN Authority including:

- Operational information – to support service management processes, enable multi-supplier investigations and ensure swift resolution to issues.
- Network monitoring data – to support security monitoring and protection of HSCN.
- Services and estate data – to enable an accurate view of the estate to be maintained and support the tracking of migration activities.
- Cost summaries – to support financial and benefits reporting.
- Service level performance summaries – to monitor performance; allow issues to be identified and performance to be published.
- Consumer feedback data – to support marketplace improvements.

Details of CN-SP reporting requirements, including data topics and frequencies, is included within the HSCN Obligations Framework and supporting Service Management Addendum.

5 Appendix: Background – Commercial Viewpoints

This section describes the commercial viewpoints documenting the interactions between the Business Capabilities described in Section 3. This information was removed from Section 4 and retained in this Appendix for background information.

- Governance Regime:
  - Outline governance approach to manage and control the HSCN services.
- Commercial Model:
  - Funding Model;
  - Contracting Model; and
  - Compliance Process.
- Marketplace:
  - Procurement support;
  - Procurement routes; and
  - Marketplace information.

5.1 Governance Regime

This section provides a set of governance principles that underpin the delivery of the HSCN services articulated in the previous sections.

An initial governance structure was developed in consultation with suppliers and wider stakeholders, as HSCN services were introduced. In order that these governance arrangements remain effective they are reviewed periodically, in consultation with stakeholders, to identify improvements, changes or efficiencies and be modified accordingly.

All suppliers will provide relevant information where required under the HSCN Obligations Framework and will have the opportunity to attend governance forums.

There are four key areas where HSCN governance will be used to direct and manage the delivery of services:

Steering Level	**Strategy**	• Strategic direction for further HSCN enhancements and transformation, including Internet First (through NHS Digital's Network and Connectivity Programme)
Operational Level	**Service Management**	• Assure the end-to-end services are being delivered as expected; • Ensure the suppliers contractual and financial performance is managed in accordance with the relevant agreements; • Support the Networks and Connectivity Programme to monitor and manage major changes to HSCN; • Ensure all delivered services comply with relevant Service Management policies and standards; • To oversee the coordination of service delivery across all suppliers; • To identify and action areas for improvement; and • To monitor service performance and conduct formal service reviews with contracted service providers.

	Security and Information Assurance	• Ensure all delivered services comply with relevant Information Security / Assurance policies and standards; and • Oversee the Information Assurance governance strategy.

Each area has:

- An agreed set of forums, which bring together appropriate stakeholders and provide focus around specific terms of reference;
- Responsibility for assessing and making decisions within the respective terms of reference, and for resolving any disagreements or other issues that arise; and
- The ability to escalate to the level above it, as indicated in the table above.

5.2 Commercial Model

5.2.1 Funding Model

The HSCN programme created a vibrant telecoms marketplace for organisations delivering health and social care. To do this the HSCN funding arrangements were predicated on supporting consumer choice in a multi supplier and multi procurement channel environment. HSCN Consumers are empowered to procure and fund connectivity services direct from HSCN CN-SP's.

The flows were therefore designed to enable HSCN Consumers to fund their access connectivity services directly, connecting to HSCN Authority-funded national services, as follows:

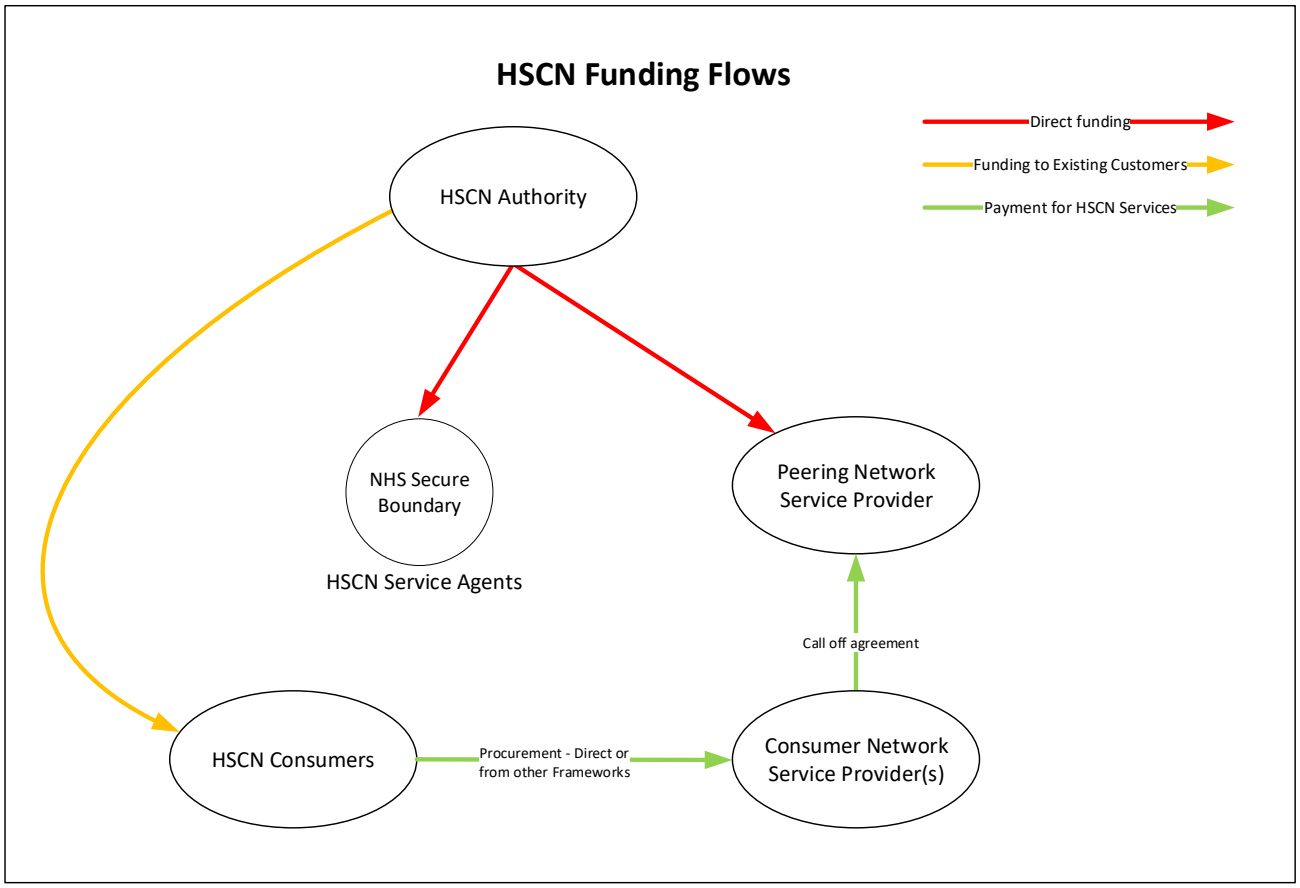

Figure 4: HSCN Funding Flows

N.B. As per section 5.2.1.2 the HSCN Business Case the HSCN Authority ceased providing funding to consumers and as of November 2020 all payments had been processed to HSCN consumer under the arrangement.

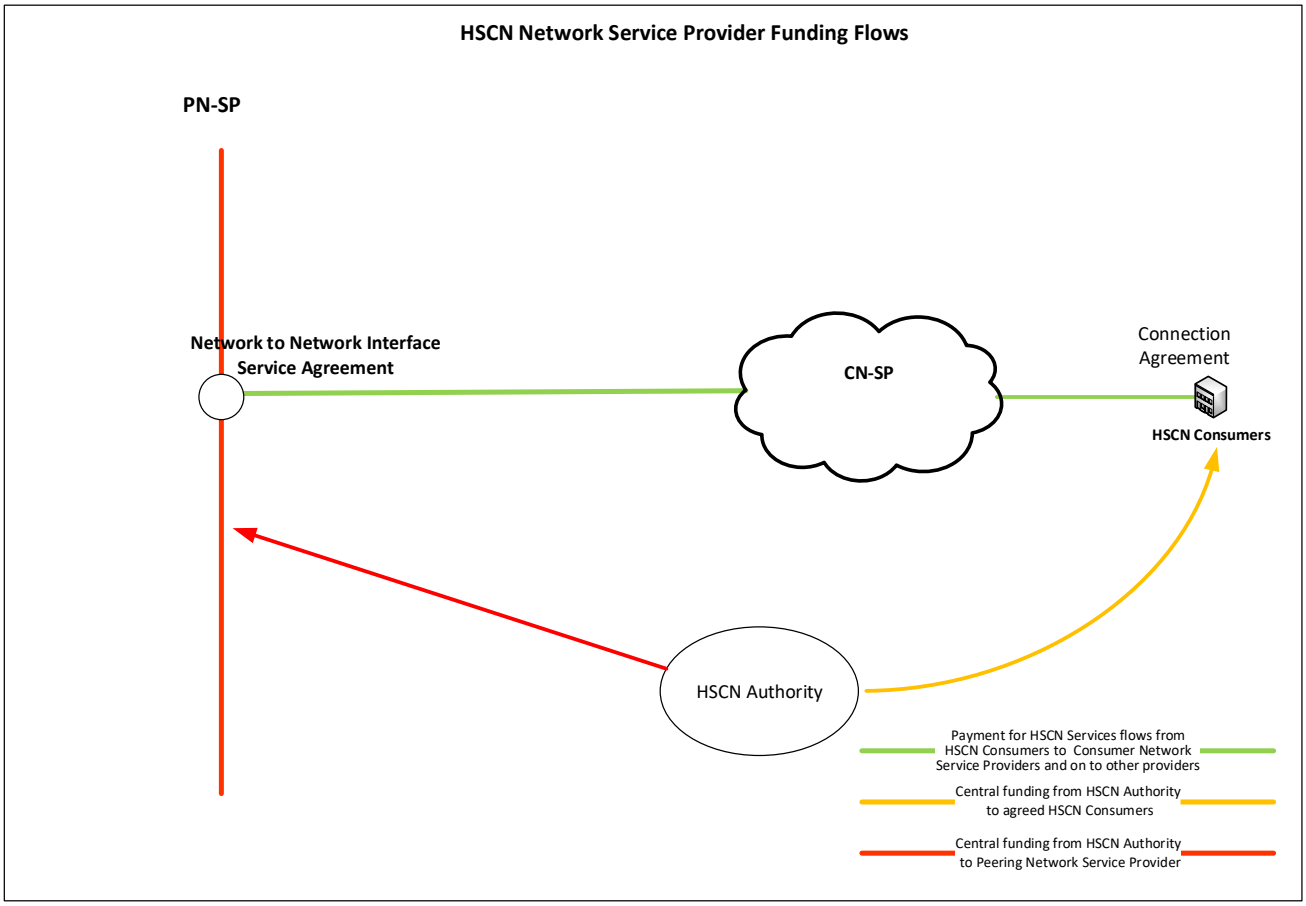

Figure 5: HSCN Network Service Provider Funding Flows

5.2.1.1 Consumer Network Service Providers

CN-SPs compete for business in the HSCN marketplace by offering competitively priced HSCN network services. CN-SPs can also differentiate offerings, varying their services by:

- Alternative service wraps, and
- Integration with other products and services they offer.

HSCN Consumers are empowered to procure HSCN connectivity services directly from CN-SPs.

5.2.1.2 Funded Consumers

In December 2016 the Digital Delivery Board approved the provision of a limited and tapering contribution towards the ongoing cost of WAN connectivity to NHS organisations over the lifetime of the HSCN business case to 2020/21. The HSCN devolved funding contribution for different organisation types is outlined below.

5.2.1.3 GP funding

The funding contribution for GP connectivity is assured as part of the General Medical Services contractual commitment to fund GP IT costs. Prior to 2017/18 this was centrally funded by the Department of Health and Social Care (DHSC). From 2017/18 it has been delegated to CCGs with 2017/18 allocations in line with the legacy N3 costs that are now payable directly by CCGs.

In 2018/19 the funding contribution provided for GP connectivity was based on:

- service costs associated with legacy wide area network (WAN) connectivity expected to remain in place throughout 2018/19
- service costs associated with HSCN connectivity expected to have replaced legacy WAN connectivity during 2018/19
- a contribution towards HSCN set up costs
- the number of GPs a CCG covers

Funding in 2019/20 is on the basis outlined above for 2018/19.

Post 2020/21, GP allocations will be increased recurrently for HSCN costs, following completion of all migration activity, and will thereafter receive annual uplifts in line with the rest of primary care allocations.

5.2.1.4 CCG funding

Whilst the funding contribution for corporate administration flows through the CCG baseline allocations, the Department of Health and Social Care (DHSC) has historically made a discretionary contribution to the cost of certain types of network to NHS organisations.

In December 2016, the Digital Delivery Board approved the provision of a limited and tapering contribution towards the ongoing cost of WAN connectivity to NHS organisations over the lifetime of the HSCN business case to 2020/21. This funding will flow non-recurrently through the CCG baseline allocation.

This tapering contribution is designed to provide a financial incentive for organisations to move away from more expensive legacy services and to provide transitional financial support as the system moves to a position where network connectivity is funded solely from CCG baseline allocations, as per other utility services.

In 2018/19 the contribution was based on:

- an equitable contribution (based upon your historic N3 costs) towards service costs associated with legacy WAN connectivity
- an equitable contribution towards service costs associated with HSCN connectivity
- a contribution towards set up costs

Funding in 2019/20 will be on the basis outlined above for 2018/19.

5.2.1.5 Trust funding

Whilst the funding contribution for trust activity is provided via commissioners through local or the NHS national tariff, the Department of Health and Social Care (DHSC) has historically made a discretionary contribution to the cost of certain types of WAN connectivity to NHS organisations.

In December 2016, the Digital Delivery Board approved the provision of a limited and tapering contribution towards the ongoing cost of WAN connectivity to NHS organisations over the lifetime of the HSCN business case to 2020/21.

This tapering contribution is designed to provide a financial incentive for organisations to move away from more expensive legacy services and to provide transitional financial support as the

system moves to a position where network connectivity is funded solely from tariff (as per other utility services).

In 2018/19 the contribution was based on:

- a fair share contribution (based on historic N3 costs) towards service costs associated with legacy WAN connectivity
- a fair share contribution (based on business volumes) towards service costs associated with HSCN connectivity
- a contribution towards set up costs

Contribution in future years will cover the same points above and will be determined each year during central business planning processes based on affordability.

5.2.1.6 Other Consumers

Other HSCN consumers, including private organisations and central & local government bodies, will not receive a central funding contribution for their service, but will also be able to procure HSCN services via CN-SPs.

CN-SPs will sub-contract as necessary with other third parties for services and act as the prime supplier for the HSCN Consumer.

CN-SPs will pay the PN-SP for connectivity services to route their HSCN traffic to other CN-SPs.

Note that all CN-SPs will stand up their own services at their own cost; recouping revenue by selling services to HSCN Consumers

5.3 HSCN marketplace

This section considers:

- HSCN Consumer support leading up to a procurement;
- Procurement routes; and
- On-going information about services that are available.

5.3.1 Procurement support

HSCN Consumers are able to access support from the HSCN Authority to assist them through the procurement of services. The HSCN Authority works with Crown Commercial Services to provide expert support in this area.

Support services include:

- General advice about network services for HSCN Consumers with limited technical knowledge, e.g. descriptions of services, procurement guides, migration guides;
- Information into predicted future trends, to help HSCN Consumers choose services suitable for current and future needs;
- Information about funding available, for qualifying health organisations;
- Sign posting to design services, for HSCN Consumers who need to contract for more detailed design advice;

- Sign posting to the various procurement routes, including online resources for those routes; and
- Sign posting to HSCN Compliant supplier details.

5.3.2 Procurement routes

HSCN Consumers were able to procure HSCN services via HSCN compliant suppliers using a variety of routes.

Aggregated procurements

To support HSCN Programme migration activities the main route was a series of centrally managed procurements for Aggregated Deployments to support timely migration to HSCN connectivity.

The HSCN Programme managed this process on behalf of organisations, especially those with existing legacy connections.

These procurements were delivered at a regional level to encourage delivery of local joined up services.

Self-Serve procurements

Organisations able to design and manage the procurement of HSCN compliant network services themselves.

This was done in collaboration with the organisations they interacted with most frequently in order to deliver health and social care services or as an individual organisation.

These could be procured via a number of routes:

- Network Services 2 RM3808: existing Crown Commercial Services Network Services Framework – suppliers on this framework may sell network services to public sector HSCN Consumers if they are HSCN Compliant;
- OJEU;
- Agreement between existing suppliers and HSCN Consumer organisations to change existing arrangements. Organisations or communities with existing networks are able to modify their existing contracts to include HCSN Mandatory Supplemental Terms. This option is only possible if the current supplier is HSCN Compliant;
- Directly from CN-SPs, for example third party commercial organisations may use this route for connection to HSCN; and
- Other Frameworks. Such as but not limited to G-cloud or RM3825

The various CN-SPs undertake activities such as product development and management; and determine what products and services they sell to HSCN Consumers. These are marketed via various routes appropriate to how they may be procured; for example, the CN-SP may offer them as standard services on RM3808 digital marketplace or via their own websites for direct awards.

5.3.3 Contracting Model

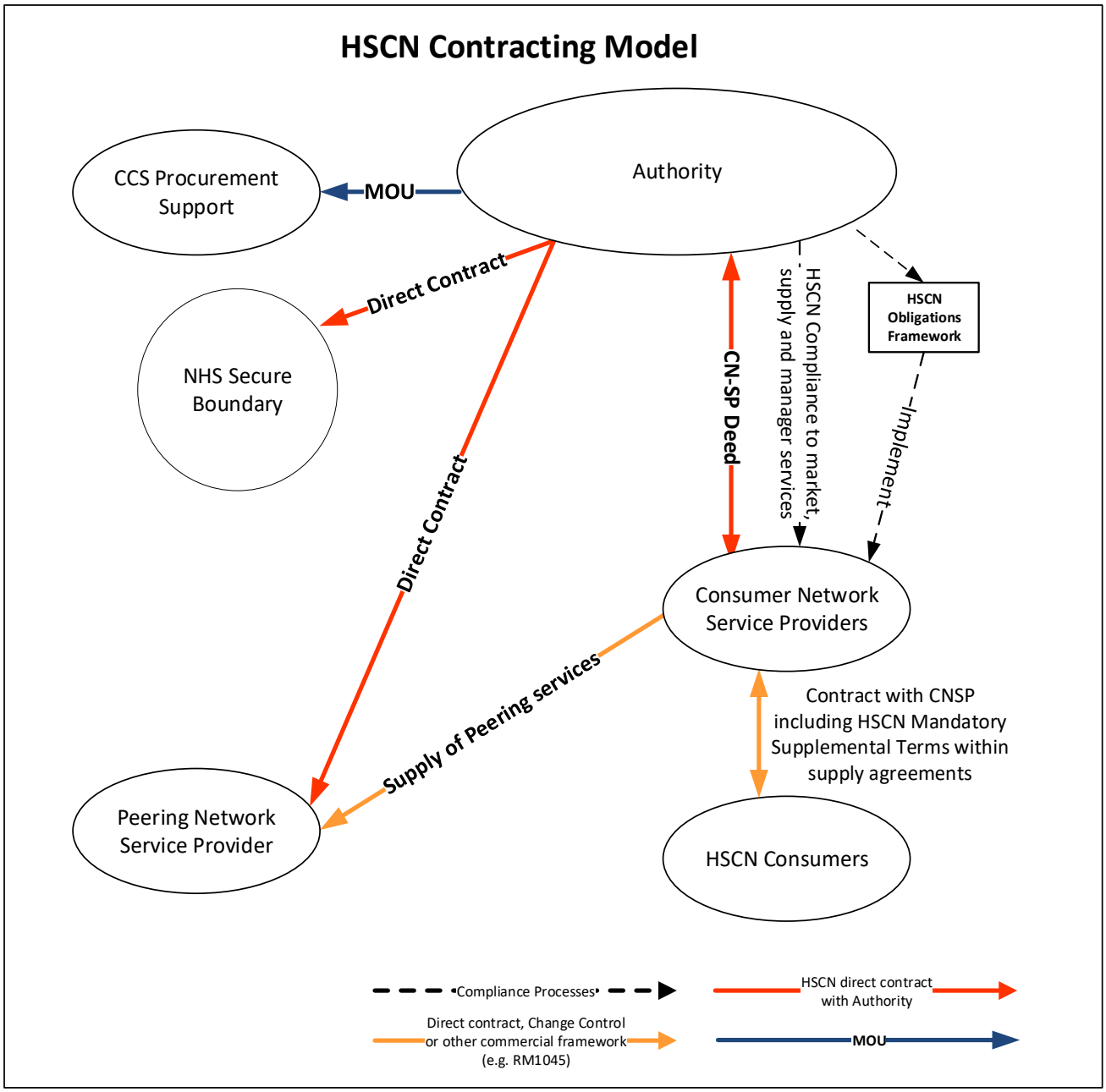

Figure 6: HSCN Contracting Model

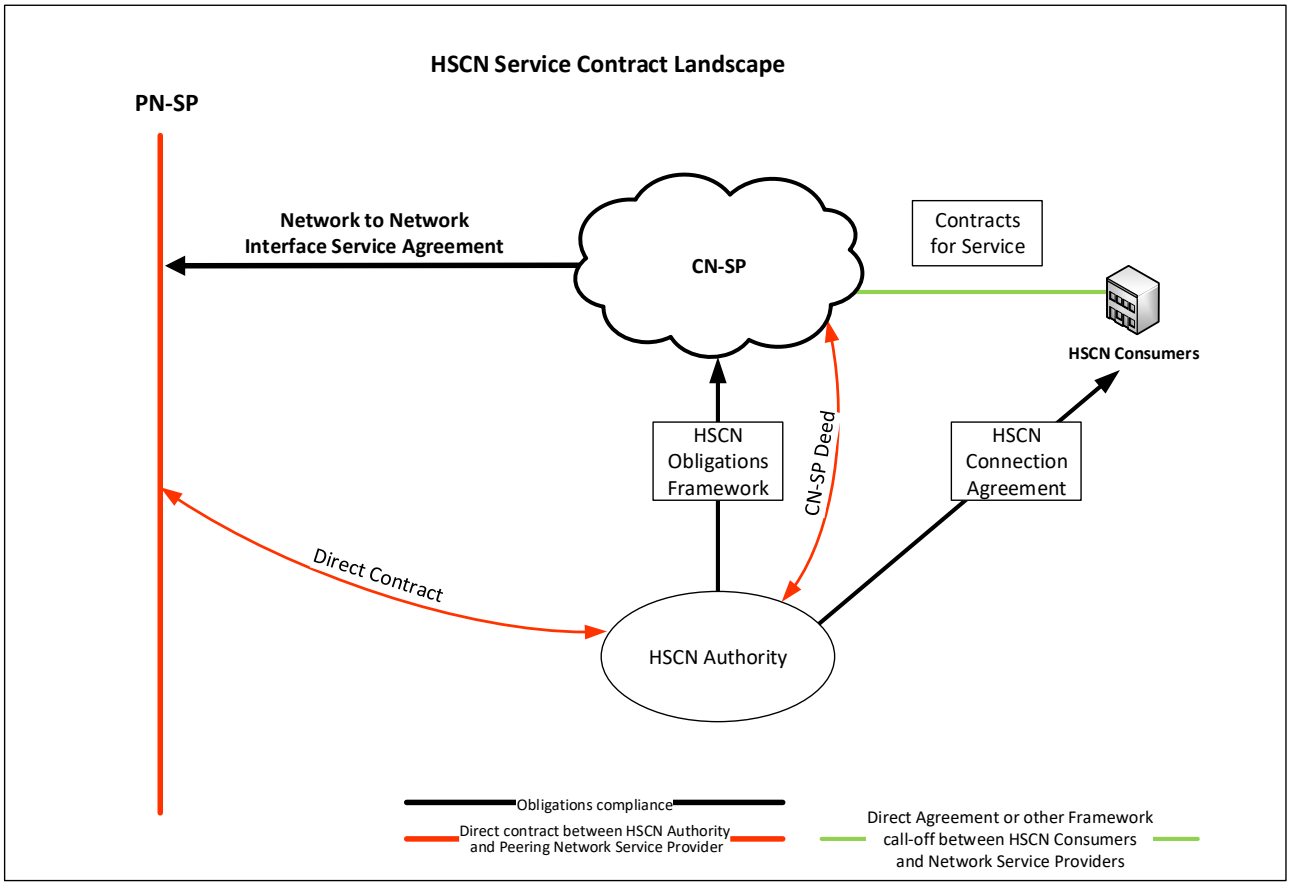

Figure 7: HSCN Contracting Flows

5.3.3.1 HSCN Authority Contracts

HSCN operates with centrally contracted services between the HSCN Authority and HSCN Service Agents and National Network Service Providers.

In addition, the HSCN Authority and each CN-SP sign a CN-SP Deed, which forms a legally binding agreement between the parties. The purpose of the CN-SP Deed is to enable the HSCN Authority to monitor CN-SP service provision and to initiate appropriate remedial activity if required. It does not replace the contractual relationship between a CN-SP and the HSCN Consumer or any contractual relationship between CN-SPs required to deliver HSCN services to an HSCN Customer.

The CN-SP Deed can be found on the HSCN website.

5.3.3.2 HSCN Consumer Contracts

Delivery of HSCN Services to HSCN Consumers are locally contracted between a Consumer and a CN-SP.

All CN-SP services are covered by the HSCN Obligations framework, by inclusion of the HSCN Mandatory Supplemental Terms in the Consumer Contract.

HSCN Consumer Contracts include a condition that CN-SPs can only supply them with HSCN services if they are HSCN compliant and that it has not been “revoked”. This condition also applies to renewal/extension of consumer contracts.

5.3.3.3 HSCN Obligations Framework

HSCN operates in accordance with the HSCN Obligations Framework, which principally covers a set of HSCN Obligations that include adherence to Policies and Standards for:

- Operations and Governance – Behavioural, Commercial;
- Technical and Security – Network controls, monitoring and Security controls; and
- Service – Service management, Testing and Assurance.

For more information on the Obligations, please refer to the CN-SP Obligations Framework, published on the HSCN Website.

5.3.3.4 HSCN Authority direct contracts

In order to ensure an integrated and coherent operation across the multiple HSCN Suppliers, the following service providers operate in accordance with the relevant operational obligations from the HSCN Obligations Framework, which will be enacted through their direct contracts with the HSCN Authority. These relevant operational obligations have been included in the centrally held contracts.

- Peering Network Service Provider; and
- NHS Secure Boundary Service Agent.

The above services demonstrate compliance with their requirements via the assurance and audit review of delivery conducted by the HSCN Authority.