HSCN Solution Overview

Version 5.0

Published 20 September 2021

Contents

Table of Figures

Copyright © 2021 NHS Digital

1. Scope of this document

This document provides an overview of the HSCN solution.

Further information about the operational design and the HSCN Capabilities that will deliver the services is detailed in the ***HSCN Operational Design Overview***. This is available on the NHS Digital website.

The HSCN Solution is summarised to enable all stakeholder groups to understand:

- What technical services are being supplied as part of the HSCN; and
- How the HSCN services will replace the incumbent services.

So that:

- The HSCN Programme Board can, on behalf of Department of Health and Social Care, assure that the HSCN Solution meets the strategic requirements;
- The Programme can confirm that the HSCN Solution meets requirements;
- Consumers understand what the replacement technical solution for their current service will be;
- Suppliers can understand the technical capabilities they will deliver.

This document details the approach for the transition of services from the Transition Network (formerly known as the N3); maintaining seamless continuity of network services and transitioning to new supplier services. The longer term strategy for network delivery is detailed in NHS Digital's Internet First Policies and Guidance.

This document includes as follows:

Section 1	Document Purpose	This section
Section 2	HSCN Overview	An overview of the HSCN and its key objectives
Section 3	HSCN Architecture	An overview of the HSCN Architecture that describes the scope of the services to be delivered. This includes an overview of the separate network components that connect the HSCN together. Includes descriptions of the network components. The architecture detailed in this section represents the Target State for the new service.
Section 4	HSCN Consumer Solutions	A brief description of the services that HSCN Consumers will receive.
Section 5	HSCN Obligations Framework	A brief description of the HSCN Obligations Framework that governs the technical and operational inter supplier working of the HSCN Components to deliver the network services required.
Section 6	Appendix: Background - Transition Network Scope	An overview of the Transition Network (formerly N3). The Transition Network is now closed but this section has been left in the document to provide background.

Copyright © 2021 NHS Digital

1.1 Reader pre-requisites

None, though the Solution Overview should be read in conjunction with the Operational Design Overview. This is available on the NHS Digital website.

2. HSCN Overview

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

"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 and information at the fingertips of clinicians, health and care professionals and citizens"

The HSCN programme was established by the Department of Health (DH) in July 2014 to:

- Manage the exit from the N3, the contract for which ended on 31 March 2017. The N3 contract was superseded by a two phase approach:
    - 1) The Transition Network
    - 2) The Continuing Orders programme
- Provision successor services to those currently provided under the N3 contract;
- Establish a network solution capable of supporting the evolving health and social care landscape.
- Manage the migration to successor services; and provide a transition path to fulfil NHS Digital's Internet First strategy

The scope of the investment covered English NHS-funded healthcare providers, including public and private organisations that were covered within the scope of N3 provision, and social care providers in England. Network connectivity for Scotland, Northern Ireland, Wales and the Isle of Man to the English private network can be accommodated should they wish to continue to access the network for as long as it is available.

The user scope for private networking has developed significantly since the original N3 business case in 2004, which focused principally on healthcare organisations. With the introduction of the Health and Social Care Act 2012, health and social care is provided through a wide range of organisations, including councils, other local government bodies, and charities and voluntary organisations who all need access to the private network.

HSCN provides a reliable, efficient and flexible way for health and social care organisations to access and exchange electronic information. By reducing cost and complexity, standardising networks, enabling service sharing and extending the parameters of collaborative working in different organisations, it saves money, enables information to be reliably shared and helps staff work together in more effective and efficient ways.

HSCN provides the robust yet flexible foundation layer upon which transformed health and social care services can be built. HSCN supports a world where anyone involved in the delivery of health and social care services can access the information and services they need to do their job from any location at any time and without the need for complex, bespoke and expensive ICT arrangements.

HSCN is designed to support the aspirations set out by the Department of Health and NHS England through the Five Year Forward View and National Information Board – Personalised Health and Care 2020 as well as NHS Sustainability and Transformation Plans, Local Digital Roadmaps and the Internet First initiative. These strategies cite increased levels of collaboration

Copyright © 2021 NHS Digital

and integration between health and social care providers as essential to driving improvements and efficiencies. Improved information sharing and the ability to work flexibly to deliver joined up health and social care services to citizens and patients are common features across all these initiatives. The HSCN programme puts in place the underlying standards, infrastructure and services that benefit the wider integration of health and social care; including, DNS Internet perimeter security and standards for Cloud connectivity. The policy regarding Cloud Services and Cloud connectivity can be found on the NHS Digital website here.

HSCN has created a marketplace for numerous suppliers to compete to deliver standardised, interoperable, better, faster and cheaper connectivity services to health and social care providers. By devolving both the responsibility and the funding for commissioning HSCN connectivity services, it empowers NHS organisations to buy what they need from their chosen suppliers and in collaboration with both NHS and non-NHS delivery partners.

The stated spending objectives within the FBC are as follows;

- Support the move from the TN to a new service whilst ensuring future innovation and a transition path to fulfil the Internet First initiative is built in
- Provide integrated connectivity to enable wider health and social care organisations to access national health IT services.
- Deliver a more efficient 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.
- A shorter contract length that enables more regular market testing to drive down costs.

The HSCN Solution enables the programme's spending objectives; foremost of which is:

> *"Support the move from the TN to a new service whilst ensuring future innovation and a transition path to fulfil the Internet First initiative is built in."*

It does this by delivering the following technical solution services:

- Establishment of a disaggregated, multiple provider network architecture;
- Defining the HSCN Obligations Framework that will require the HSCN services to meet the HSCN Obligations, Policies and Standards;
- Defining HSCN Obligations, Policies and Standards that enable safe, reliable and efficient interoperability;
- Establishing an HSCN Compliance Operating Model to allow multiple network service providers to offer HSCN Services that meet the HSCN Obligations;
- Enabling a more open marketplace with multiple providers and increased local empowerment for consumers to choose HSCN services;
- Supporting the creation of virtual 'Community of Interest' or 'Regional' networks where the majority of collaboration and data sharing will take place;
- Reducing the size and cost of a centrally provided private core network, whilst continuing to support national applications and services that need the availability and performance of a private network;
- Bringing disaggregated Internet provision within the scope of a layered security monitoring approach to support a longer-term strategy of reducing the reliance on private networking;
- Improving the cyber defence capability by the provision of active cyber defence capabilities included within the service supplementing the activities carried out by the Data Security Centre – please see HSCN Operational Design Overview;

Copyright © 2021 NHS Digital

- Delivering a controlled and stable migration from TN services to the replacement HSCN services

3. HSCN architecture

3.1 Introduction

The architecture detailed in this section represents the HSCN Target State that supported the migration from Transition Network services; and to provide a transition path to fulfil the Internet First initiative to reduce the reliance on private networking and move to a wholly internet-based provision.

This section details the HSCN Components and the approach that was adopted to migrate Transition Network services to this architecture.

3.2 Architecture principles

The following principles underpin the network architecture:

- The HSCN architecture will be "open" to all Health and Social Care users and their partners with a valid need to connect without favour and on an equal access basis;
- The HSCN architecture will not constrain or mandate the number of network service providers in any way, subject to network service providers compliance to the HSCN Obligations;
- No HSCN service provider shall be able to technically constrain or block any other HSCN service provider;
- The HSCN will incentivise the use of the internet in preference to private networks, except where business requirements dictate otherwise;
- HSCN will provide the capability to support fixed, mobile and remote access by its users;
- HSCN will support IP based applications and services (e.g. multi-media voice, video and data);
- Designs will include adherence to GDS Network Principles;
- HSCN will be available 24hrs a day, 7 days a week for 365 days per year; and
- HSCN will provide security controls at the network layer to protect its own security, integrity and availability as a transport mechanism.

Copyright © 2021 NHS Digital

3.3 Logical Network Topology

3.3.1 HSCN Target State

The following diagram outlines the HSCN target state.

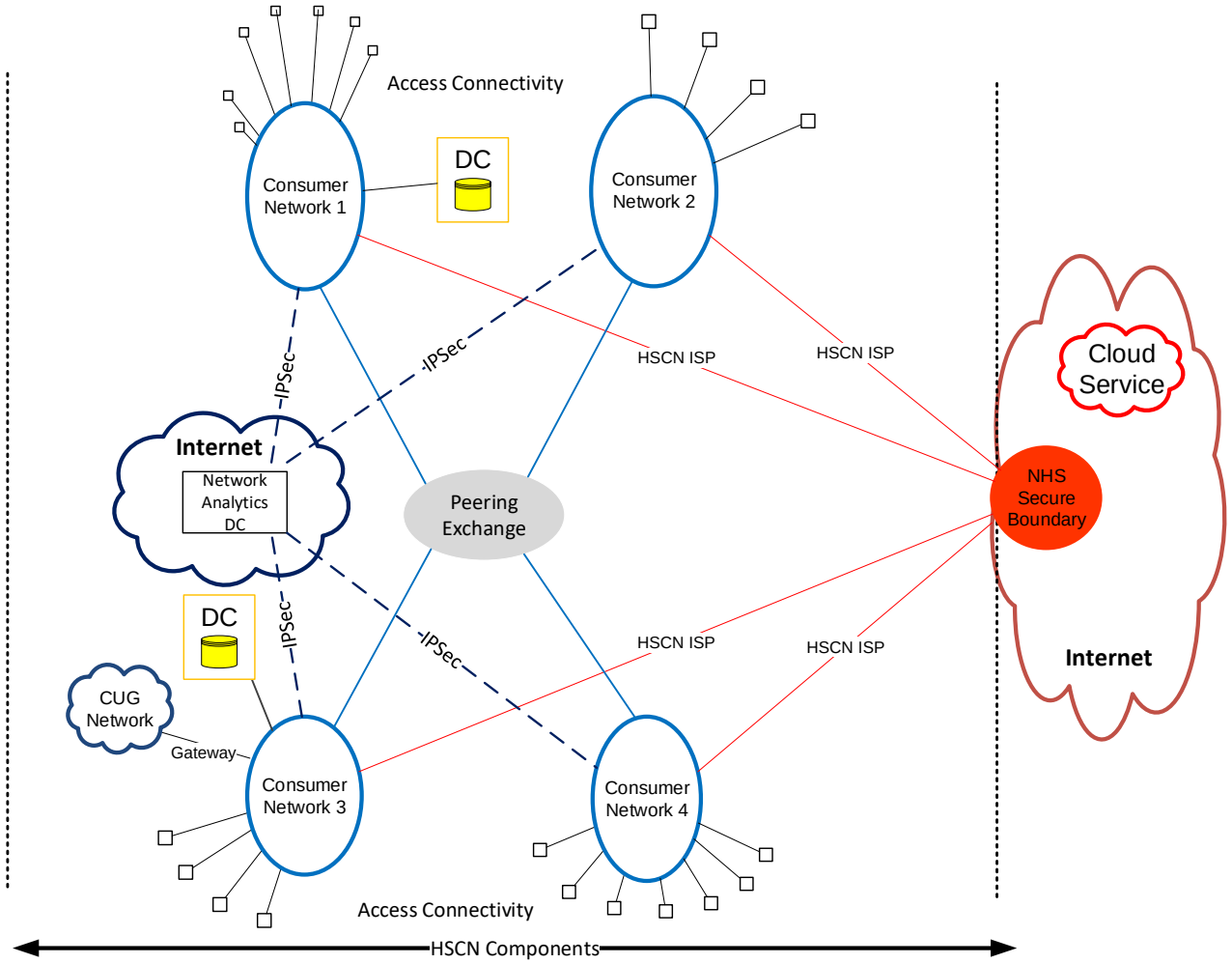

Figure 1 - Target State

3.3.1.1 HSCN Components

The HSCN consists of the following Components:

- A number of **Consumer Networks (CNs)** that provide WAN routing between HSCN endpoints and access connectivity for end sites [note diagram has only 4 for illustration purposes]:
  - HSCN Access Connectivity for individual sites/organisations (e.g. NHS Hospitals, Primary Care, Community & Mental Health, Clinical Commissioning Groups (CCG), Care Homes, 3rd Parties) to the Consumer Network (CN).
  - These services are offered to HSCN Consumers directly including the end to end service through the Peering Exchange Network and other HSCN end

Copyright © 2021 NHS Digital

points. The HSCN Consumer is required to complete an appropriate HSCN Connection Agreement in order to receive this service.

- Provide aggregation and virtual routing of HSCN traffic flows between CN end points, including as examples:
    - To/from national applications
    - Public routing to/from the Internet via provision of Internet Service Provider gateway (HSCN-ISP)
    - Inter-site routing (application access, point to point data sharing).
- A Consumer Network Service Provider (CN-SP) can deliver the HSCN network services once they have achieved HSCN Compliance
- The CN-SPs provide the end to end service for HSCN Consumers including security, technical, delivery and service management responsibilities.
- CN-SPs may offer a range of network services from basic access circuits to full network provision (e.g. private WAN services, Voice over IP, Video Conferencing and Cloud services).

- **Peering Exchange Network (PN)**:
    - Support all routing across the HSCN disaggregated networks including as examples:
        - To/from national applications
        - Inter-consumer Network routing.
        - Flexible and rapid path to connectivity / interconnectivity
        - Level playing field across the disaggregated supply of CNs
        - Simplified end-to-end Service Assurance & fault diagnosis
        - The PN services will be delivered by the Peering Exchange Network Service Provider (PN-SP) on the behalf of NHS Digital.

- **Data Security Centre**:
    - Provides a monitoring and alerting capability, collecting and centrally collating information from all parts of the HSCN Components. The information is used to support central security oversight of HSCN.
    - Provide cyber threat management to support the protection of the HSCN service overall from threats originating both externally and internally.
    - Manage the following components:
        - **Network Analytics Service (NAS) -** ingesting network telemetry data to perform proactive and reactive analysis on the data in order to identify any malicious activity taking place over HSCN.
        - **NHS Secure Boundary Service–** filtering of outbound and returned internet traffic to manage cyber threats**.**

Copyright © 2021 NHS Digital

3.3.1.2 Business Application Services

The HSCN supports the delivery of key Business Application Services to provide value added business applications that exploit the IP network e.g., Voice / Collaboration / Video / Secure Remote Access. Network transit for these services is over HSCN; but the services in themselves are not part of HSCN supply chain.

These services are not shown on the diagram, as they are not part of HSCN delivered Components and Technology Services; but are included here as a description to illustrate the applications and services that exploit the network.

Delivering these services is not subject to the HSCN Obligations; therefore, they may be provided by any supplier and are not restricted to suppliers who have achieved HSCN Compliance. They can be purchased off relevant Lots on frameworks such as the CCS Network Services Agreement (RM3808) or as direct contracts.

CN-SPs may offer these services to HSCN Consumers blended with HSCN services and with a service wrap that supports seamless service management. For example, CN-SPs may offer HSCN connectivity with consumer procured services such as voice and remote access; with one helpdesk provided for all delivery.

The HSCN service provides interoperability guidance to allow HSCN Consumers to purchase these applications that will be compatible to run over the HSCN. Guidance documentation and consumer support services will be provided to support implementation.

Business Application Services may be delivered over the internet direct and not connected to HSCN. This approach follows the Internet First Initiative. These applications will still be subject to Information Governance standards for data handling and security. Each party needs to be aware of their responsibility as either a data controller or data processor if appropriate. HSCN Consumers can access these via the Internet outbound service provided under HSCN (referred to as the NHS Secure Boundary Service).

3.3.2 HSCN Traffic Flows

The HSCN Access Connectivity will be provided with HSCN specific traffic flows across the Consumer Network. This will enable enterprise business flows, including to national services and the internet.

Three open traffic flows will be supported by CN-SPs as standard:

- Routing to the internet direct from the CN-SP ISP services (via the Secure Boundary) – known as HSCN-ISP Flow; and
- Routing to other HSCN end points; end points on the same CN, and end points on other CNs via Peering Exchange Network – known as HSCN-Standard Flow.
- CN-SP's shall facilitate routing to the Public Sector Network (PSN) from the CN-SP – known as the PSN Flow. Where the CN-SP already has a PSN relationship, for example is a Direct Network Service Provider (DNSP) then the interface can be provided directly by the CN-SP. Otherwise the CN-SP will need to partner with an organisation who has that direct PSN relationship.

Copyright © 2021 NHS Digital

Other virtual closed user group mechanisms (inc. Routing and VRFs) can be supplied on CNs to support regional private sharing of data if required. These are not pre-built for consumers, and so will require design and extra implementation to support requirements. These can be used for community of interest data sharing between partner organisations.

The following diagram shows the interconnection routing flows:

- Red represents public traffic to the Internet – HSCN-ISP Flow
- Blue represents routing of traffic to other HSCN Consumers on the same CN or other CNs – using HSCN- Standard Flow.

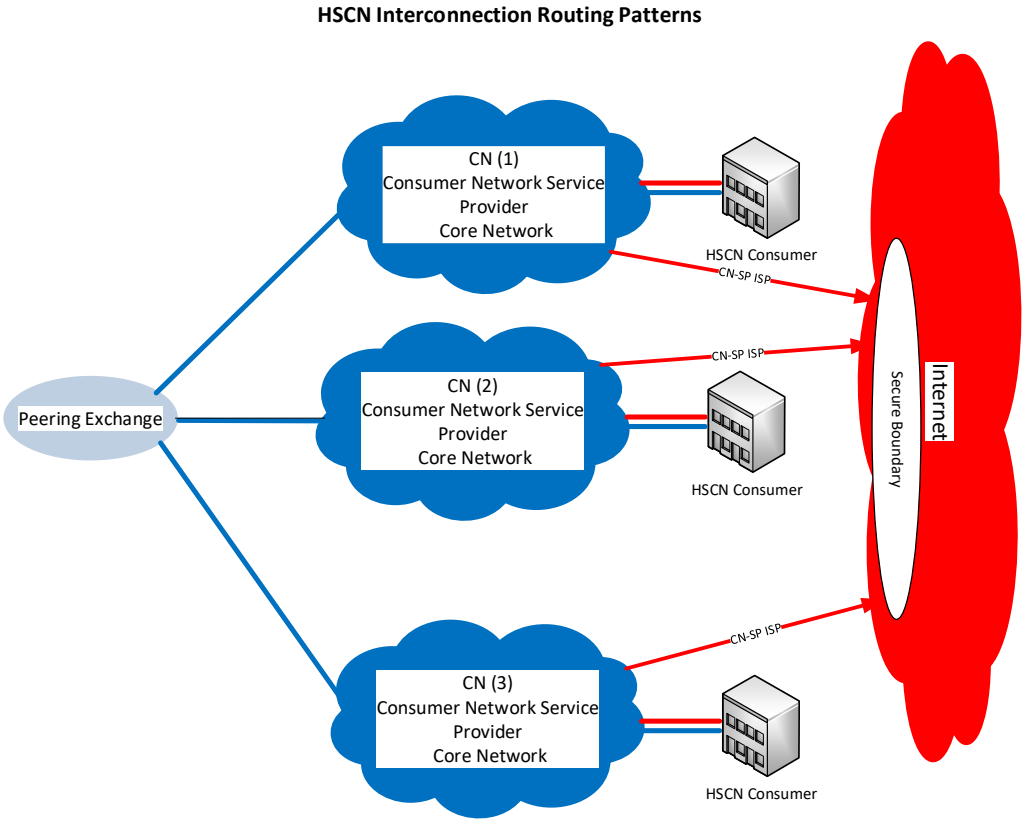

Figure 2 - HSCN Interconnection Routing Patterns

Copyright © 2021 NHS Digital

As an illustration, the following example business flows that will be supported by each CN are as follows:

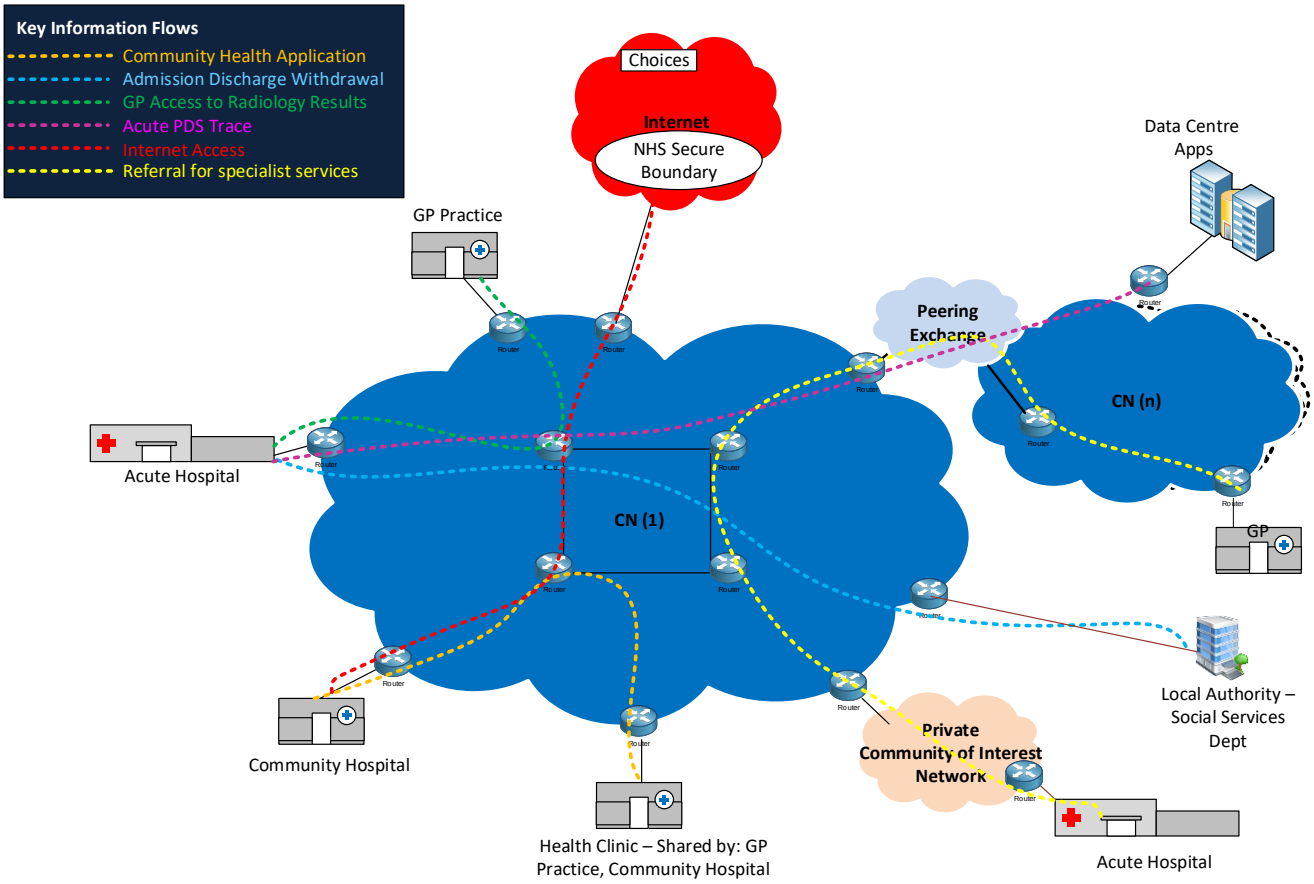

Figure 3 - HSCN Traffic Flow Examples

Business Flow	Examples in diagram	Routing approach
HSCN National Applications flow	Acute PDS Trace to Spine PDS service	HSCN national traffic flows across the CN and routed onward to the HSCN CN that hosts the data centre where Spine is located. Uses HCSN-Standard Flow via Peering Exchange Network. HSCN CN routes to the Spine connected data centre (PDS Service).
Internet Access	NHS Choices website access	HSCN public traffic flow across the CN and routed onward to NHS Digital's NHS Secure Boundary Service via the CN-SP ISP where it then breaks out to the internet 'proper'. Uses HCSN-ISP Flow. CN-SPs provide internet breakouts as a separate ISP service to end consumers.

Copyright © 2021 NHS Digital

Cross and Inter CN data sharing – data flows that are not closely coupled services	Referral for specialist services (e.g. to specialist hospitals)	The HSCN flows traffic in an open network to other connected HSCN endpoints as standard functionality. Data flows between organisations that are not grouped together as a closed user group will use the HCSN-Standard Flow. This will be supported by cross CN flows to all HSCN endpoints and inter CN routing over Peering Exchange Network. Note it is also expected that most of these flows over time will be managed at an application level for example, via eRS or other interoperability options.
Health and social care data sharing – shared commissioned services for closely coupled health communities	GP access to Acute Radiology service NHS-Social Care Admission / Discharge / Withdrawal Community Health Application	User defined application sharing requirement. Utilises consumer defined closed user group routing (or VRF) for greater security and consumer control. These flows are typically regional data sharing and often delivered via COINs in current models. Procured by the health economy from their HSCN CN-SP. These are closed user group services for a group of Health and Social care end organisations. For this to be delivered efficiently the organisations in the user group should be connected to the same CN, but they could also be extended across CNs if required.

3.3.3 HSCN Component Characteristics

3.3.3.1 Consumer Networks (CNs)

A number of **HSCN Consumer Networks (CNs)** support HSCN Access Connectivity and routing across HSCN. These are delivered by CN-SPs on their existing network acting as aggregator, contact point, control and administration between services supplied to HSCN Consumers.

Consumer Networks 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, and 3rd Parties etc).

HSCN Consumer Network service providers (CN-SP) for all their HSCN network services – are the direct service provider to HSCN Consumers and work with other suppliers (CN-SP and PN-SP) to manage the service end to end. HSCN CN is supplier agnostic in concept, by enabling and utilising an open market.

CNs provide the routing between sites connected to that CN and onward forwarding of traffic to the internet, Cloud Service Providers, 3rd parties and other CNs via the Peering Exchange Network.

The CNs support a range of connectivity and routing patterns, to allow regional virtual private networks combined with the HSCN traffic flows.

Network Service Providers are able to offer CN-SP services after gaining the required HSCN Compliance.

Copyright © 2021 NHS Digital

Characteristics:

Access Connectivity	A variety of access configurations including: o Resilient Diverse – diversely routed access circuits connecting to two CN PoPs o Resilient – diversely routed access circuits to one CN PoP o Non Resilient – single access circuit connecting to one CN PoP Blended access technology offered included but not limited to the following: ▪ ADSL2 ▪ Fibre to the Cabinet (FTTC) ▪ Fibre to the Premises (FTTP) ▪ Ethernet (offering a range of bandwidths; 10Mbps, 25Mbps, 60Mbps and 100Mbps Committed Data Rate (CDR) to meet Organisation requirements ▪ Flex Ethernet – (offering a range of bandwidths; 200Mbps, 300Mbps, 500Mbps,1Gbps, 10Gbps) ▪ 3G and 4G Wireless Mobile Connections Gateway to PSTN / National Cellular networks managed as network-to-network interfaces. Note that these are to be provided for the delivery of voice business applications and are not mandatory. Regional Data Centre gateway connectivity for third parties hosting applications consumed by HSCN Consumers including Business Application Services. Dual-stack Architecture is mandatory to support transition to IPv6.
Core network	Open traffic flows for HSCN connected services that are fully resilient and diversely routed Dispersed PoPs Dual-stack Architecture is mandatory to support transition to IPv6 Resilient connection to the HSCN Peering Exchange Network
Routing	Examples of potential routing options: • Closed user group virtual networks for logical grouping of sites and user organisations based on function (e.g. Primary Care), organisational (CCG and commissioned services), regional or a combination of these. • Simple HSCN connectivity for consumers who are agnostic of regional sharing and requiring only the HSCN-Standard Flow to other HSCN end points, to national applications and HSCN-ISP Flow to the internet.

Copyright © 2021 NHS Digital

ISP Services	ISP services that meet the security monitoring required in the HSCN Obligations Framework: • Provision of security monitoring and management services to provide resistance to malicious attack and monitor usage. • Routing of all public traffic to/from the Internet via HSCN NHS Secure Boundary.
HSCN Technical & Security Obligations	Compliance to HSCN Technical and Security Obligations as per the HSCN Obligations Framework. Included, but not limited to: • IP Addressing • DNS • QoS • Security / IG • Network Monitoring and Security management - including monitoring the internal CN providing outputs to the Network Analytics Service to support network monitoring across HSCN.
HSCN Service Obligations	Compliance to HSCN Service Obligations as per the HSCN Obligations Framework. Included, but not limited to: Management capability for end to end performance issues (consumers and other HSCN Network Service Providers) Service performance reporting.

3.3.3.2 Peering Exchange Network (PN)

Supports all routing across the HSCN disaggregated networks including as examples:
- To/from national applications
- Inter Consumer Network routing.

The PN services are delivered by the Peering Exchange Network Service Provider (PN-SP).

Characteristics:

Interconnectivity	Provides two Peering Exchange locations at geographically diverse Carrier Neutral Provider locations in London and Manchester. A highly available solution that provides an uncontended interconnection between all HSCN CN-SPs. Interconnectivity between all HSCN CN-SPs will be open and unrestricted. The peering exchange uses route servers to provide appropriate routing capabilities for the scale of the network. The peering exchange will be capable as an option of hosting multiple logical networks such as VPN and VRF technologies.

Copyright © 2021 NHS Digital

Connections for CN-SPs	Provide resilient connection of up to 30 CN-SPs initially. Provide two connection options at 1Gbps and 10Gbps. Shall provide published and guaranteed service levels for CN-SP requested capacity including provision of all required interfaces. Manage the on-boarding and disconnection of Consumer Network Service Providers, including on-site engineering in the peering exchange facilities. Each Consumer Network Service Provider connected to the peering service shall be provided with its own exclusive interface at both peering exchange locations.
Service	Operate a 24x7x365 network operations centre to monitor and manage the peering exchange service. The peering exchange will have monitoring and maintenance tools that are accessible to NHS Digital and CN-SPs such as utilisation monitoring and a looking glass service. Comply with the necessary HSCN Obligations. The peering service will be subject to and maintain adherence to NHS Digital IA requirements including physical and logical security controls to secure the peering exchange infrastructure and management tools as amended from time to time by change control. ISO27001 compliance is mandatory requirement.

3.3.3.3 Data Security Centre

Cyber Security is provided via a layered security approach with oversight by the Data Security Centre service consisting of the following:

- CN-SP Security Management;
- Network Analytics Service (NAS);
- NHS Secure Boundary Service (NHS SBS);
- Firewall protection controls, including; IP Blacklist implementation and NHS Digital provided blocked addresses.

Further detail on the operations of this service is included in the HSCN Operational Design Overview.

Network Analytics Service (NAS)

The Network Analytics Service (NAS) supplements 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.

Further detail on the operations of this service is included in the HSCN Operational Design Overview.

Copyright © 2021 NHS Digital

NHS Secure Boundary Service

HSCN Consumer Network Service Providers will direct all Internet bound traffic towards the NHS Secure Boundary Service. Outbound and returning inbound HTTP internet traffic will be subjected to the NHS Secure Boundary Service's processes.

The NHS Secure Boundary Service identifies and blocks known malicious activity and resources, including:

- Malware;
- Zero day malware;
- Worms;
- Viruses;
- IP Addresses and URLs; and
- botnet traffic.

The NHS Secure Boundary Service provides NHS Digital with logging and reporting, with events and reports to be specified by NHS Digital.

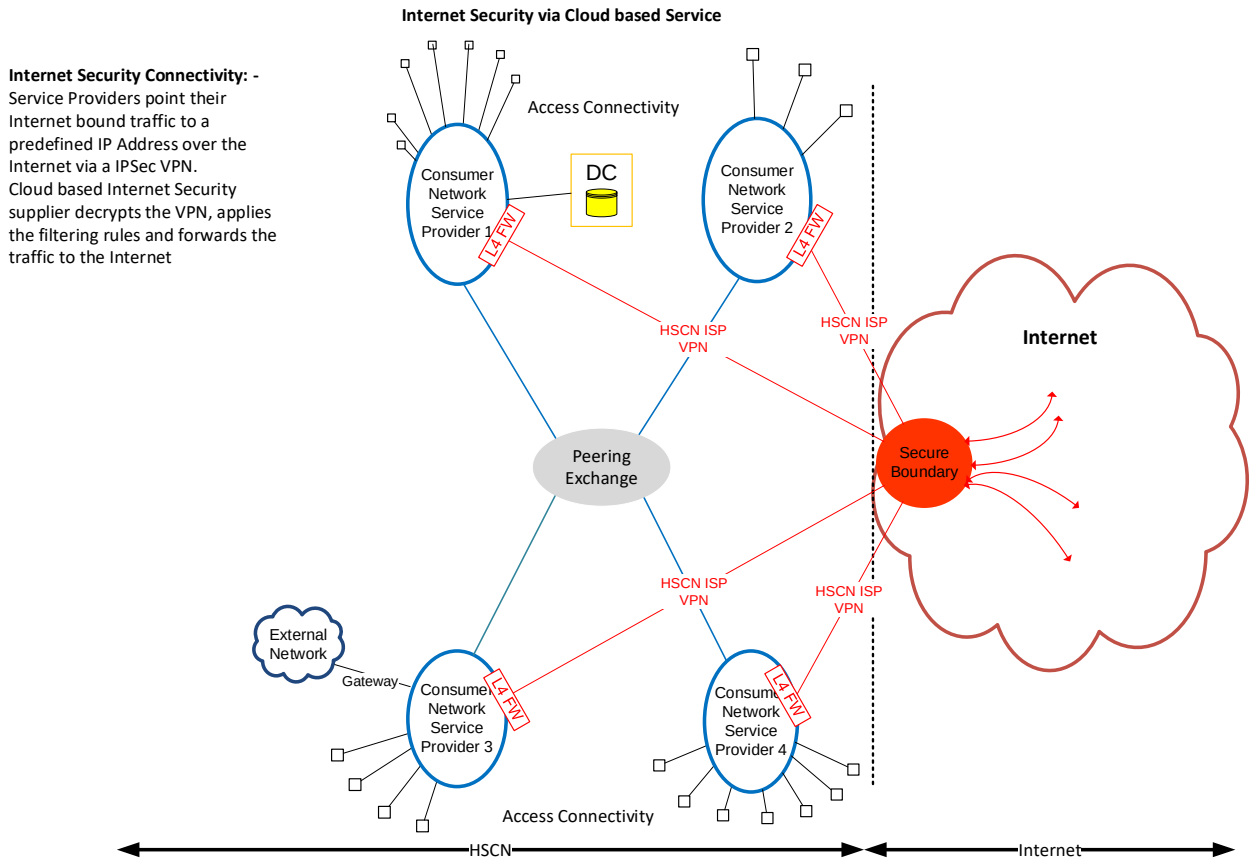

Figure 4 - HSCN NHS Secure Boundary Service

Data Security Centre

The Network Analytics Service (NAS) and the NHS Secure Boundary Service reporting feeds into the NHS Digital's Data Security Centre service.

The Data Security Centre service ensures that Cyber Threats and Incident Management is undertaken with the correct people, process and technology.

Copyright © 2021 NHS Digital

Data Security Centre Capabilities include:

- Incident Management (Internal)
- Investigation of SIEM alerts
- Management of NHS Digital Security Policy
- Monitoring of NHS Digital Physical Security
- Support into NHS Digital CareCERT for:
  - National Broadcast Functionality
  - Threat Analysis & Triage
  - Health & Care System Incident Management.

Data Security Centre supports CareCERT by supplementing the following functionality:

- Provides incident response expertise for the management of cyber security incidents and threats across the health and care system.
- Broadcasts potential cyber threats and suggests remedial actions to over 10,000 contacts in health and care, helping organisations protect themselves.
- Is a central source of security intelligence for health and care, working with cross government partners such as GovCertUK and CERT-UK.
- Supports the analysis of emerging and future threats through unique analysis tools and reporting.
- Provides insight for decision makers to help shape departmental strategy.
- Is a trusted source of security best practice and guidance.

3.3.4 HSCN Technology Services

Each of the HSCN Components includes, as appropriate, Technology Services to support the requirements of data exchange between end points and across the HSCN and are key enablers to the delivery of applications and systems.

Interoperability Services

Use of services and standards for configuration are required for interoperability, and the implementation requirements are included in the HSCN Obligations to deliver a consistent end to end service for the following:

- Domain Name Service (DNS)
- IPAM (IP Address Management)
- Quality of Service (QoS).

Note that the HSCN Obligations include adherence to HSCN Policies and Standards for these services e.g. the NHS IP Addressing Policy. The HSCN Authority IP Address Management service allocates IP Addresses to the HSCN Consumer. The CN-SP will set up IP addresses for their connected customers, supported by IP Address Management processes.

Security and Network Monitoring

In addition, the HSCN Obligations include technical obligations to support network monitoring and monitoring of cyber incidents.

Cyber incidents will be managed by the Data Security Centre.

The CN-SPs capture IPFIX telemetry data at points within their network capable of representing each consumer's CPE device. Regardless of where the IPFIX data is collected it must be possible to determine the organisational source of the data upon analysis. As the telemetry data is

Copyright © 2021 NHS Digital

collected it is ‘exported’ to the NAS where the data will be aggregated, analysed and reported upon.

The following diagram details the security telemetry flow on the HSCN Service:

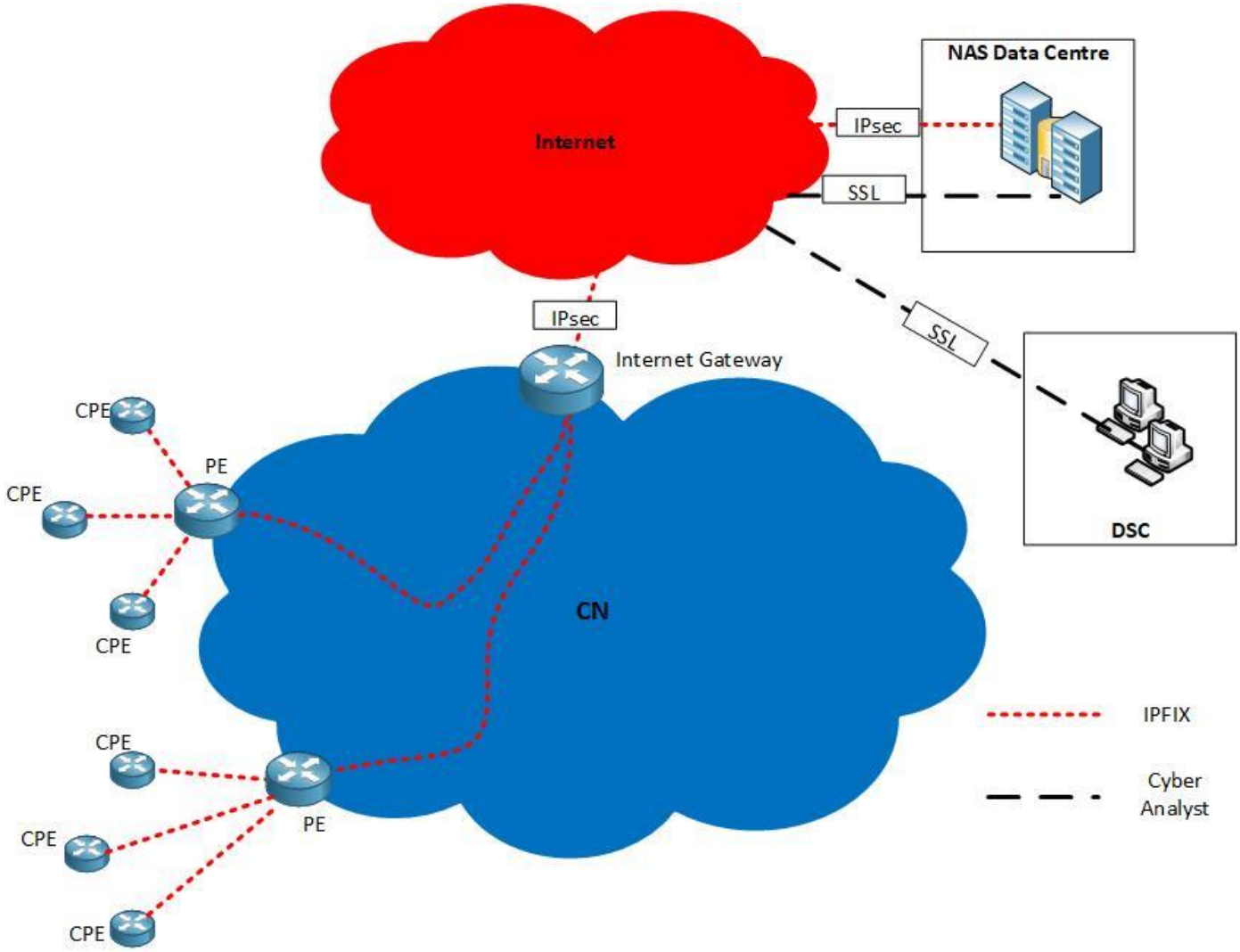

Figure 5 - Security Telemetry Flow

Obligations have been made on service providers delivering HSCN services to ensure that the specified information flows (e.g. IPFix) representative of the CPE boundary points are provided to the NAS.

The NAS service aggregates the telemetry data, perform a deduplication process and then analyse the information based upon analysis rules created by the Security Cell team.

Copyright © 2021 NHS Digital

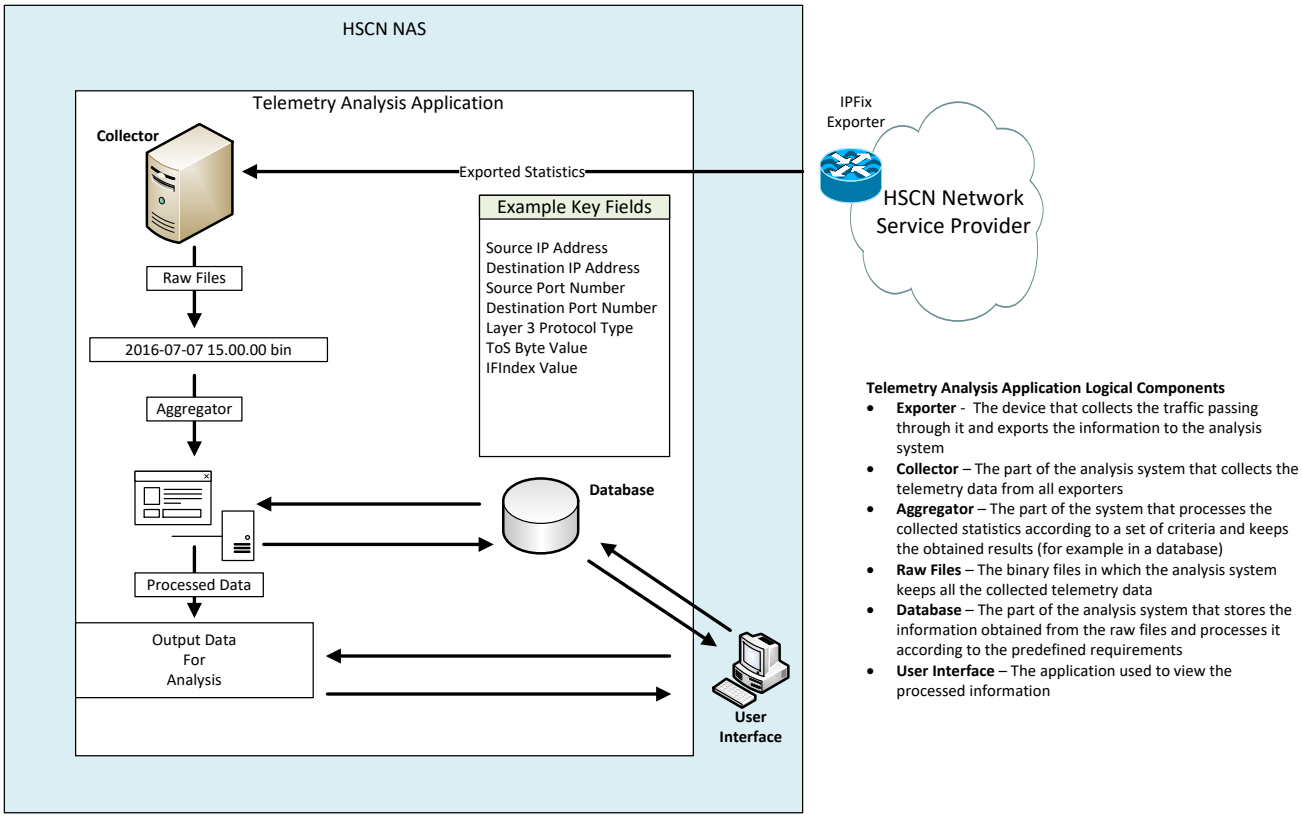

Figure 6 - Security Monitoring Points

In addition, the service providers deliver security and network monitoring on their internal networks.

Note the security controls delivered as part of the Data Security Centre service or as security HSCN Obligations on the Network Service Providers does not provide end to end security of applications and devices. As a set of security principles:

- HSCN does not provide security controls at higher layers on behalf of connected users or connected end-systems (i.e. to organisations, applications or data centres); the customer and application provider should instead ensure appropriate security controls are in place to protect those users, systems and data.
- Confidentiality should be provided entirely within connected end-systems, not by the HSCN network.
  HSCN should not be used as the sole authentication/authorisation control to grant access to data and services.
  HSCN does not prevent data from being conveyed to and processed on an inappropriate end-user device. The suitability of different HSCN-connected devices (desktops, laptops, tablets, smartphones, etc.) to handle different data sets is a matter for end systems (users and application providers), not for HSCN.

Copyright © 2021 NHS Digital

4. HSCN Consumer Solutions

Consumer Network Service Providers may choose to offer a range of options to HSCN consumers that encompass the end to end access and distribution layer service.

- **Managed** – Fully end to end service for HSCN Access Connectivity from consumer premises to an HSCN CN end points, with HSCN routing across the enterprise including the routing required to connect across the CN to National Applications on the HSCN and the Internet.
- **Gateway** - HSCN gateway connections to other external networks/aggregators that are controlled connections. These are a specific form of access connectivity that includes managed secure boundaries between an external network and the HSCN.

Elaborated example patterns of service offerings will be provided by the HSCN Programme on the HSCN website.

HSCN Consumers will be able to source services in several distinct ways; please see HSCN Operational Design Overview for further details.

Services must only be procured from HSCN Compliant CN-SPs.

Copyright © 2021 NHS Digital

5. HSCN Obligations Framework

The interoperation of the HSCN Components is underpinned by a set of HSCN Obligations to support end to end operations.

CN-SPs are assured against a set of obligations that ensures they work to requirements for interoperability. Where required, HSCN Policies and Standards will be developed to provide definitive detail on implementation. HSCN Compliance will be awarded to CN-SPs by undertaking the assurance process detailed in the HSCN Compliance Operating Model which can be found at https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers.

The HSCN Obligations that apply to the CN-SPs can be found at https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers. The HSCN Obligations will include, but be not limited to:

- **Operations and Governance** – operating procedures and controls, including
    - Network Service Provision such as collaborative working and CN-SP Deed signature
    - Governance Regime including as governance forums and reporting
    - Compliance Process including assessment, evidence and renewal
    - Connection Agreement
- **Technical and Security** – These include, but will not be limited to:
    - DNS
    - QoS - requirements for Quality of Service and end-to-end assurance as appropriate
    - IPAM - to work within (or address) known constraints and limitations, such as IP addressing
    - Routing protocols and principles
    - Network monitoring
    - Security - controls and integrated monitoring
        - Provide security controls at the network layer of each of the technical components to protect its own security, integrity and availability as a transport mechanism.
- **Service Management** – These include, but will not be limited to Service Intervention in relation to:
    - Service Integration;
    - Service Standards;
    - Incident Management;
    - Change Management;
    - Release Management;
    - Service Improvement;
    - Network Monitoring; and
    - Performance Management.

Copyright © 2021 NHS Digital

6. Appendix: Background - Transition Network services

6.1 Introduction

In order to fully understand the scope of the HSCN programme it is necessary to understand, at a high level, the nature of the now decommissioned Transition Network provision in terms of the technical capabilities that currently support the Health and Social Care connectivity needs.

The boundary of scope for the HSCN Programme has been established to enable the programme's strategic objectives, foremost of which is:

> *"Support the move from TN to a new service whilst ensuring future innovation and a transition path to fulfil the Internet First initiative is built in."*

This section provides details of the scope of the Transition Network technical services.

6.2 Transition Network scope

N3 provided a high quality, fully managed, Wide Area Network (WAN) and had over 40,000 direct, virtual and aggregated connections. These services consisted of direct access connections, VPN connectivity and connections that linked to N3 via an Aggregator.

April 2017 saw the expiry of N3 contract, which was replaced by the BT Transition Network and the Continuing Orders programme.

The Transition Network service was managed as a run-down solution as clients and services were migrated off of TN. For example, Legacy Access circuits were ceased and re-provided as HSCN Access Connectivity from CN-SPs.

The Transition Network contract allowed the migration to HSCN to be planned in a controlled manner that supported continuity of service for Legacy N3 connections.

6.2.1 Transition Network (TN)

The Transition Network (TN) supported the Legacy N3 products and services during their migration to HSCN and provided:

- Core Network functionality that supported the management and routing of network traffic within the TN, connecting Points of Presence (PoPs) and supporting external Gateways
- Access PoPs that supported Legacy N3 Access Services
- Head End services, Broadband, Video Conferencing (VC) and Virtual Private Network (VPN), that supported Legacy N3 Services
- Enhanced Internet Gateway (EIG) that consisted of an Internet Gateway, Enhanced Monitoring Service (EMS) and Advanced Behavioural Analysis Suite (ABAS)
- Security Management Services
- Connectivity to the Transition Network was available to HSCN users via the Peering Exchange. This allowed HSCN users access to Legacy N3 applications and services on the TN.

The figure below demonstrates how the Transition Network provided optimal use of assets to provide continuity of service during migration to HSCN:

Copyright © 2021 NHS Digital

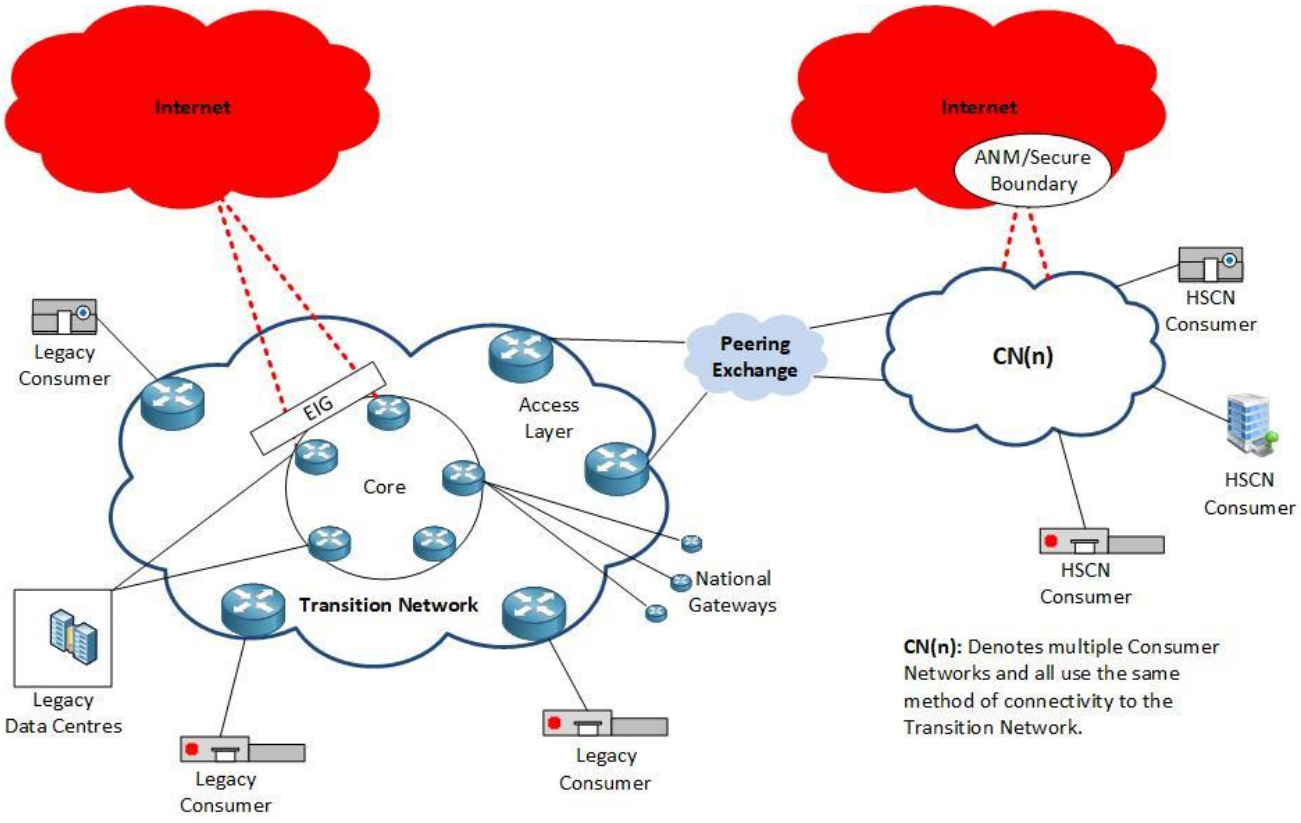

Figure 7 – Transition Network Logical Topology

The design and key aims of the Transition Network were to provide a stable and flexible infrastructure to maintain support for remaining N3 applications and services and to support the legacy N3 clients during migration to HSCN.

6.2.2 Transition Network components

The transition Network was made up of two main layers

- The Core
- The Access Layer

The Transition Network hosted the Legacy N3 components whilst facilitating their migration to either HSCN or the internet.

6.2.2.1 Transition Network core

The core layer was responsible for providing interconnections between:

- The Points of Presence (PoPs) in the Access Layer
- Gateways to the internet and a Multi-Protocol Label Switching (MPLS) service
- Connectivity for Legacy N3 Services, including Legacy Data Centre services
- The Core Network, Peering Connection Service and the HSCN Peering Exchange Network

Copyright © 2021 NHS Digital

6.2.2.2 TN Access Layer

The Access Layer included a number of chargeable PoPs that provided Network access to the TN. Each PoP was resiliently connected to the core via ethernet.

Each PoP provided support for ethernet and private circuit based Legacy N3 Access Service.

The Access Layer also acted as the bearer interface for legacy VPN services and legacy Broadband services.

PoPs were subject to continual review with the objective of decommissioning PoPs when no Legacy N3 Access Services remained connected to them or under the specific retirement conditions.

6.2.2.3 Head End services

- **Broadband**: This allowed TN End Users of the broadband Legacy N3 Services to continue to utilise their existing links to connect to the TN Service whilst they migrated to HSCN.
- **This VPN Head End** allowed all TN Consumers of a VPN Legacy N3 Service to continue to utilise the service until they migrated to HSCN. This VPN Head End consisted of a managed central infrastructure. The central infrastructure and associated internet connectivity provided the remote access services, including Firewalls, switch, routers, VPN concentrators and authentication services.
- **Enhanced Internet Gateway:** The Internet Gateway service provided TN End Users with outbound connectivity to the internet and included a firewall and URL filtering service
- **Video Conferencing Head End:** This service allowed TN consumers continued use of the legacy Video Conferencing service until migration to HSCN. It provided:
    - Secure connection to the Video Conferencing management service.
    - Managed Video Conferencing Bridge. The managed bridge was inside the TN with connectivity to both the TN and the internet. This provided an online tool for booking and scheduling meetings along with a central directory of all registered video conferencing units
    - Central ISDN Breakout. This feature enabled communications with other Video Conferencing users still on ISDN.
- **HSCN Peering Connectivity Services:** The HSCN Peering Exchange Network is independently contracted by the NHS Digital, who contract with the Peering Service Provider for use of this service.

6.2.2.4 Legacy services

Legacy services consisted of services that were resident on the N3 and were migrated either to HSCN or transitioned to the internet (including Cloud Services). These included several Clinical Services applications.

Copyright © 2021 NHS Digital