Document filename:	**Data Security Centre Services Directions 2020 Specification**		
Project / Programme	**Data Security Centre**	Project	
Document Reference	**QMS9136**		
Project Manager		Status	**Final**
Owner		Version	**2.0**
Author	REDACTED	Version issue date	**16/03/2026**

Data Security Centre Services Directions 2020 Specification

Document management

Revision History

Version	Date	Summary of Changes
2.0	16/3/2026	Redacted for publication

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
REDACTED	IG Lead, PTT (Delivery and Ops), NHS England	03/02/2026	V1.2
REDACTED	IG Lead, NHS England	30/1/2026	V1.2
Kevin Willis	Head of Information Law, NHS England	4/2/2026	V1.2
REDACTED	Higher Executive Officer	17/2/2026	V1.2

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Mike Fell	Executive Director Cyber Operations, NHS England	02/03/2026	1.2
Phil Huggins	National CISO for Health & Care, Department of Health and Social Care	02/03/2026	1.2
Jackie Gray	Direction of Privacy and Information Governance, NHS England	12/3/2026	1.3
Ming Tang	Chief Data and Analytics Officer, Interim Chief Information Officer, NHS England	16/3/2026	1.3

Glossary of Terms

Term / Abbreviation	What it stands for
DSC	Data Security Centre
CSOC	Cyber Security Operation Centre
SIEM	Security Information Event Monitoring
ATP	Advanced Threat Protection

HSCN	Health & Social Care Network
WAF	Web Application Firewall
IOC	Indicator of Compromise
TIP	Threat Intelligence Platform
SOAR	Security Orchestration, Automation and Response
TN	Transition Network

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of document

This document sets out the specifications for the information to be collected and analysed by the NHS England's Data Security Centre[1] in performance of the services it provides or offers to the health and care sector. The document should be read alongside the Data Security Centre Services Directions 2020 issued by the Secretary of State for Health and Social Care (**the Secretary of State**).

Introduction

The Secretary of State charged NHS England with creating the Data Security Centre to support health and care organisations to be more cyber resilient and respond to incidents promptly when they happen, working with the National Cyber Security Centre.

The Data Security Centre Services Directions 2020 provide a basis for NHS England to provide services and support that achieve the following security principles for the health and social care sector:

- Manage security risk.
- Protect against cyber-attacks.
- Detect cyber security incidents.
- Minimise the impact of cyber security incidents.

NHS England will support the achievement of these principles in a number of ways such as assuming the role of a Managed Security Service Provider (MSSP), or by issuing advice and guidance, or by providing implementation tools and assurance. Collectively, the services and support provided by NHS England are the Data Security Centre Services (**the Services**) described below, which will be provided to organisations within the Inclusion Criteria below.

Area of Operation for the Specification Document

England only - **Eligible organisations** - those that meet the criteria to receive the Services include:

- Arm's-length bodies of the Department of Health and Social Care:
    - Executive agencies, which are legally part of the department.
    - Special health authorities, which can be created by legislation and are subject to direction by the Secretary of State.
    - Executive non-departmental public bodies, whose relationship with the department is defined in legislation.

[1] https://digital.nhs.uk/cyber

    - Advisory non-departmental public bodies and expert committees, which form part of the core of the department.
    - The Department's remaining arm's-length bodies, which take a variety of other forms.

- Local Authorities providing Adult Social Care.
- Primary Care:
    - Dentists.
    - GP's.
    - Pharmacy.
    - Urgent care services, including NHS 111 and GP out-of-hour services.
    - NHS funded online primary care.
- NHS Trusts and Foundation Trusts:
    - NHS Acute Trusts.
    - Ambulance Trusts.
    - Community Health Trusts.
    - Mental Health Trusts.
- Independent health and care providers providing NHS or local authority funded care.
- Specialist healthcare 'edge' cases where NHS data is being used, for example;
    - prisons
    - young offender institutions
    - secure settings
- Any other organisation that has access to NHS patient data and systems.

Data Protection Impact Assessments (DPIA)

A DPIA exists for each component/service, sub service and platform, that processes personal data detailing the legal basis, purpose, and description of processing. The assessments demonstrate how fairness is measured, with the governance and assurance controls to ensure that the data complies with data policy and standards, not only of NHS England. The assessment includes the retention periods of each platform and the methods through which data is deleted.

Organisations receiving the Services should perform their own DPIA upon the platforms and services they wish to adopt.

NHS Secure Boundary

The solution protects and monitors the internet traffic of the local internet breakout (when the traffic leaves the network) of **eligible organisations** (those that meet the criteria to receive the services) and the internet traffic traversing the Health & Social Care Network (HSCN) by using a cloud based next generation firewall.

This detects security threats and enables more preventative actions and controls to be used to protect systems and their associated data. A local internet breakout is the point in a network where traffic destined for the internet leaves the healthcare providers network. The rules around which traffic will only be protected and not monitored will be defined by the eligible organisation as part of the setup of the service.

The solution also provides eligible organisations with additional protection for locally hosted HTTP applications using a cloud-based Web Application Firewall (WAF). This WAF protects against common attacks and is deployed to protect a specific web application or set of web applications.

Personal data inspected and/or collected

- **Names of users -** within eligible organisations whose data traverses the network; required to allow different security policies to be applied to individual or groups of users based on their NHS organisation and role.
- **Email addresses of users** - within eligible organisations whose data traverses the network; required for email link analysis for threats such as phishing. It is also used by NHS organisations administrators to log on to the service.
- **Online Identifier e.g. IP Address/Event Logs** - required to be able to allow or block traffic based on the source or destination. It also required to allow the service to trace any malicious activity
- **Internet Browsing History** - required to investigate security incidents where an account has been compromised (i.e. Phishing) or a user has been breaching their local organisation's security policies.

In identifying and inspecting network traffic, the NHS Secure Boundary Solution may identify the following personal data:

- Address; Postcode; DOB; Age; Sex; Marital Status; Gender; Living Habits; Professional Training / Awards / Education; Income / Financial / Tax situation / Financial affairs; Physical Description; General Identifier e.g. NHS No; Home Phone Number
- Website Cookies; Mobile Phone / Device No / IMEI No; Device MAC Address (Wireless Network Interface); Banking information e.g. account number, sort code, card information; Criminal convictions / alleged offences / outcomes / proceedings / sentences

In addition, in identifying and inspecting network traffic for malicious content, the NHS Secure Boundary Solution may identify the following special category personal data:

- Physical / Mental Health or Condition – including reports and medical images.
- Sexual Life / Orientation; Religion or Other Beliefs; Trade Union membership; Racial / Ethnic Origin; Biometric Data (Fingerprints / Facial Recognition); Genetic Data

Protective Monitoring

Eligible organisations have the option to enter into a contract to use the protective monitoring service. This service provides to the customers real-time security threat monitoring, detection, and response capabilities. The service aims to identify potential security threats impacting the organisation and recommends response activities to contain, mitigate and resolve the identified security incident. The service includes threat monitoring, threat triage and threat response, as well as the support needed to ensure proper data source integration with the NHS England Cyber Security Operating Centre (CSOC) platforms.

Platforms & Toolsets

The Protective Monitoring Service utilises a number of platforms;

- Security Information Event Monitoring (SIEM)
- Threat Intelligence Platform (TIP)
- Security Orchestration, Automation and Response (SOAR)
- Incident Management Platform (IM)

The information inspected and/or collected into these Protective Monitoring platforms enables NHS England to support Health & Care Organisations with their management, investigation and remediation of any suspected or live security incident by providing specialist knowledge and skills (dependant on the incident complexity) to ensure the correct course of action is followed.

The SIEM platform captures, indexes, and corelates real time audit data in searchable repositories from which it can generate graphs, reports, alerts, dashboards, and visualisations.

The SOAR is designed to assist security teams in managing and responding to endless alarms at machine speeds. With SIEM and SOAR combining comprehensive data gathering, case management, standardization, workflow and analytics to provide the CSOC with the ability to implement sophisticated defence-in-depth capabilities.

Following the typical “Who, What and When” they can protect following types of assets against known and suspected security vulnerabilities:

- User Accounts
  - Individuals (such as compromised accounts or known insider threats)
  - Service Users (such as automated processes being ran as an individual)
- Servers
- End-user devices
  - Workstations

    - Laptops
    - Tablets
    - Smart phones & mobile devices
    - Internet of Things / Internet of Medical Devices
- Network equipment
- Installed Software
- Cloud services
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)
    - Mobile "backend" as a service (MBaaS)
    - Serverless computing
    - Function as a service (FaaS)

NHS England does this by the following analysis and linkage:

Real-time monitoring – The SIEM can identify all the entities in the IT environment, including users, devices and applications as well as any activity not specifically attached to an identity. The SIEM can then use that data in real time to identify a broad range of different types and classes of anomalous behaviour. Once identified, that data is fed into a workflow that has been set up to assess the potential risk to the business that anomaly might represent. For example, using email headers information and meta-data from NHSmail to correlate events with use-cases from the SIEM to detect the extent of a malware distribution so as to be able to respond and mitigate in as near real-time as possible.

Incident response – Incident response is controlled via a Cyber Security Incident Response Team (CSIRT) that is embedded within the CSOC function. The CSIRT operates in conjunction with other enterprise groups, such as 3rd party suppliers, public-relations and disaster recovery teams. In addition to technical specialists capable of dealing with specific threats, it includes experts who can guide enterprise executives on appropriate communication in the wake of such incidents. The CSIRT with authority would initiate the invocation of the NHS Cyber Incident Response Plan (CIRP).

As part of the development of security use case and as part of the CSOC onboarding process, playbooks are created detailing the process to follow upon an event detection. Following the verification that a security event is true, it is classed as an incident and the relevant playbook is initiated and the appropriate incident response process is followed, with evidence and tracking performed within the IM platform.

Device & User monitoring – This capability allows the CSOC to analyse access and authentication data, establish account/device context and provide alerts relating to suspicious behaviour and violations of national and local policy.

Threat Intelligence – The TIP allows the CSOC to aggregate, correlate, and analyse threat data from multiple sources in real time to support defensive actions. By importing

threat data from multiple sources and formats, correlating that data, and then exporting it into an organization's existing security systems or ticketing systems, a TIP automates proactive threat management and mitigation. The TIP uses external APIs to gather data to generate configuration analysis, Whois information, reverse IP lookup, website content analysis, name servers, and SSL certificates. Interacting with the SIEM, combined they detect the threats that are most relevant to the organisations to whom the CSOC are providing the Services.

Advanced Threat Detection – The SIEM and TIP adapt to new advanced threats by implementing network security monitoring, endpoint detection and response sandboxing and behaviour analytics in combination with one another to identify and quarantine new potential threats.

Use Case Library - The use case library spans SIEM, SOAR and TIP toolsets to help analysts to automatically discover new use cases and determine which ones can be used within their environment, based on the data ingested at the time of its ingestion. This ultimately results in the benefit of reducing risks by enabling faster detection and incident response to newly discovered and ongoing threats.

Network Monitoring - The Network Monitoring service uses the routers and gateways between the Transition Network (TN), Health & Social Care Network (HSCN) and the Internet to monitor all data transiting across each of the networks.

Data collection

The individual Data Privacy Impact assessments of the SIEM, SOAR and TIP platforms detail the data collected but as a non-exhaustive list, the following are typical types of data collected:

- **Network Traffic**
    - **Internet Traffic** primarily captured via the NHS Secure Boundary solution, this is traffic that has originated from within the NHS, the HSCN network and is routing to the internet.
    - **Inbound Traffic** is captured as Web Application Firewalls, where the network connection is originated on the internet and is routing to any NHS/HSCN source of data
    - **Traffic Metadata** – this is data about the network assets or services which have been accessed including the specific user who accessed them.
- **Authentication Data**
    - **Authentication Service Data** – the service that identifies a set of credentials against a directory, verifying the identification matches an asset and providing a role or level of access to one or more solutions. By way of example, this could be the audit of which certificate a workstation identified itself by before gaining access to a corporate network, or the username of a user and that they provided a non-captured password successfully to identify themselves to access a webpage.

    - **Directory Data** – the service matches network activity to specific users (machine and/or personal) to provide both audit and access control. For example, some users may be allowed to access a specific website while others are not. Data from an NHS organisation's local directory service (name, email, IP address) may be used to identity individual users.
    - **Authenticator Metadata** – this is data about the authentication of assets and service to service, and which directory service or additional authenticator function may have been utilised to provide authority to gain access to services.

- **Endpoint (i.e. server and workstation)**
    - **File data** - such as file names, sizes, and hashes.
    - **Process data** - running processes and hashes.
    - **Registry data** – this is a hierarchical database that stores low-level settings for the operating system.
    - **Network connection data** - host IPs and ports.
    - **Machine details** - machine identifiers, names and the operating system version.
    - **Application data (**error and event logs) – email, I.P address, machine identifiers, may include special categories of personal data within error/crash logs

Analysis and outputs

All information including processed information is made available to the originating organisation.

End-Point Security

By opting into the NHS England centralised Windows 10 agreement which includes Microsoft Defender Advanced Threat Detection (ATP), organisations benefit from better cyber security protection.

Microsoft Defender ATP is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. It can be deployed on most modern Microsoft Windows operating systems (Windows 7 and later), including servers, laptops, tablets and workstations. Additional platform support is available for macOS, Linux, Android and iOS.

With centralised ATP deployed across each respective organisation end point estate, both the organisation locally and the national CSOC can detect, alert and prevent abnormalities in real time. It provides a security lens into the threat landscape offer better detections on an organisational and national level.

Awareness and Education

Respond to an NHS Cyber Alert

The purpose of the “Respond to an NHS Cyber Alert” service is to:

- Collect up to date NHS organisational contacts.
- Collect up to date SIRO contacts for NHS organisations.
- Allow users to maintain the appropriate contact details for their organisations including mobile telephone numbers to receive high-severity alerts via SMS.
- Recording an NHS organisation's compliance of receiving and acting on a high security alert within 48 hours of the alert being issued.
- Provides reports of the compliance to NHS England regional leads.

Data collection

As part of the service, the following data are collected:

- NHS organisation (ODS) code.
- Registered user details including, name, business email address and business telephone number.
- Technical contact details including, name, business email address and business telephone number.
- SIRO Contact details including business email address and business telephone number.
- Organisations’ response to receiving a high alert - ‘Yes’, ‘No’ or ‘Not applicable’ and any other mitigation comments.

Phishing Training Tool

The purpose of the training tool is to improve staff awareness on the threat of phishing across their organisation. This is done by a cloud-based portal which is available to all health and care organisations on a voluntary basis. NHS England delivers a (harmless) simulated phishing email to a large number of individuals within an organisation and provides a report and recommendations based on the results. This simulation highlights how aware an organisation's workforce are of phishing attacks.

It is linked to a training animation that is bespoke to each of the health and social care organisations adopting this service

Data collection

Organisations will voluntary enrol themselves and provide a list of staff email addresses they want to be involved in the simulation.

Immersive Labs

This is a cyber security training platform https://immersivelabs.online/signin. NHS England has a contract with Immersive Labs under which Immersive Labs is NHS England’s Processor. NHS England provides licenses to NHS organisations to use the

site. Immersive Labs collects the personal data of NHS staff who register with the platform in order for the staff to take online cyber security training modules.

Data collection

During registration and use the following information is collected - staff name; work email address; IP address and cookie information.

Incident Management

Civil Contingencies Act 2004

The Data Security Centre provides internal incident support to NHS England, but in times of national emergency could provide incident support to the Health and Social Care sector of the UK. In such times it may be necessary to ingest log files and other machine information from local organisations which are not normally collected in order to resolve incidents.

Whilst the Civil Contingencies Act 2004 (**CCA2004**) does not apply to NHS England, the Secretary of State and NHS England are **Category 1 Responders**[2] and have duties set out in the CCA2004 (Contingency Planning) Regulations[3].

Regulation 47 enables a Category 1 Responder to request other general Category 1 Responders (e.g. NHS Trusts) or general Category 2 Responders (e.g. CCGs) to provide it with information. The information must be:

- Reasonably required to enable the Category 1 Responder to carry out its duties to assess the risk of an emergency occurring or to make contingency plans for emergencies, or
- Be required in connection with the performance of another function of the Category 1 Responder which relates to an emergency.

The request for information may only be made where the Category 1 Responder does not hold the information required and it is not reasonable to seek to obtain the information by other means. Under this Regulation the Secretary of State or NHS England could:

- Request data from NHS Trusts or Clinical Commissioning Groups under the CCA2004 (Contingency Planning) Regulations.
- Require the Trusts/CCGs to supply the necessary data to NHS England.
- Engage NHS England to collect the data under a service agreement, or if the collection is personal data, engage NHS England as a Processor.

[2] http://www.legislation.gov.uk/ukpga/2004/36/schedule/1/part/1

[3] Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 - http://www.legislation.gov.uk/uksi/2005/2042/regulation/47/made; as amended by the Civil Contingencies Act 2004 (Contingency Planning) (Amendment) Regulations 2012 - http://www.legislation.gov.uk/uksi/2005/2042/contents/made

NHS England's legal authority to collect the data would be section 270 of the 2012 Act; i.e. it would be in reliance on the legal authority of the Secretary of State or NHS England to collect the data under the CCA2004 (Contingency Planning) Regulations.

Data collection

The data collected would be dictated by the situation, the information could be derived from:

- Antivirus software (AV)
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- File systems
- Firewalls
- Routers
- Servers
- Endpoints
- Switches

Analysis and outputs

The SIEM (discussed above) essentially creates actionable information for incident response. This could either mean a dashboard displaying information in real-time or sending an alert if something abnormal is detected, in either case, the incident response team could act immediately and reduce the impact or even totally prevent a security breach from happening.

Assurance and Audit

Cyber Security Support Model (CSSM)

The CSSM has been developed to help NHS organisations increase their response and resilience to cyber security incidents, whilst supporting them in working towards the Cyber Essentials Plus accreditation and to improve their security posture overall. The elements of the model are:

- an independent assessment of an organisation's cyber security to identify and understand their risks and vulnerabilities. This will allow an organisation to make informed decisions around improving their cyber security and increase patient safety
- specialist support in the remediation of issues identified during their assessment. This will provide support in a variety of areas which could include activities such as back-up or active directory reviews
- tailored training and awareness of key roles in an organisation who are accountable or contribute to the security of an organisation. This will allow these roles to develop their knowledge and understand their obligations in adopting a cyber culture and understanding the cyber-threat landscape.

Data collection

As part of the service, the following data are collected:

- Organisational information on data security.
- Contact details on the organisation which are kept within Customer Relationship Management system.

Vulnerability Management

NHS England has a Vulnerability Scanning service which runs an external vulnerability scan which aims to identify weaknesses/holes in external facing network firewall(s) that malicious actors can exploit. External scans usually identify immediate threats to an organisation, out-dated firmware and software that could be exploited, and open ports and protocols.

- **Security Rating Service**
  Security Ratings provide an overview of a company's cyber security posture and serves as a measure of their risk (similar to a consumer credit rating). The service is non-intrusive (i.e. no penetration testing) – Externally observable data is collected from various publicly available internet sources.
- **Vulnerability Management Service (VMS)**
  The VMS solution is centred around a scanning tool. This service provides a more in-depth external vulnerability scanning option based on a list of an organisation's external facing Internet Protocol Addresses. Additionally, a vulnerability ranking service, in which a ranked report of vulnerabilities based on asset criticality and known exploitations is also available.

Data collection

Open source vulnerability information from the NHS estate.

- **Directory data** – the service matches Internet traffic to specific users to provide both audit and access control. For example, some users may be allowed to access a specific website while others are not. Data from an NHS organisation's local directory service (name, email, IP address) used to identity individual users.
- **Network connection data** - host IPs and ports.
- **Machine details** - machine identifiers, names and the operating system version.

Analysis and outputs

All information including processed information is made available to the originating organisation.

Cyber Data Platform

The purpose of the Cyber Data Platform is to provide a strategic reporting capability for the health and care sector. This is done by ingesting a limited sub-set of data from existing data sources e.g. Microsoft Defender, Phishing Campaigns, the results of security penetrative testing (PenTest), cyber incidents, Data Protection & Security Toolset, Technical Remediation, Network & Information Systems Regulations compliance, Vulnerability Management Service, BitSight and many more. The ingested

data provides a high-level summary, especially to understand trend-over-time, and provide actionable insights to authorised users.

Data collection

Personal data is collected and processed for user management of the platform purposes, including: name, business contact details (including business email address and business telephone number), organisation details, title and roles, security clearance details.

Consultation

To comply with section 258 of the Health and Social Care Act 2012, the DSC has consulted with the following:

- The Department of Health and Social Care.
- The Cyber Associates Network (CAN), representative of over 250 organisations which include Trusts, CSU's, ICB's and STP's.
- Individual trusts that agreed to participate in Data Security Centre (DSC) pilots.
- The SIGNS network which includes NHS, local authorities, universities and other types of organisation that may use the NHS England services set out in the Specification.
- Industry experts (e.g. IBM / Accenture / National Cyber Security Centre).

Dissemination/sharing

Regular dissemination/sharing

Information collected will be disseminated to:

- The local organisation where the data originated.

In accordance with section 261(2)(e), information collected and analysed will be disseminated to the following organisations to support their regulatory or advisory role, where there is a lawful basis to do so:

- The Department of Health and Social Care.
- The Care Quality Commission.
- The National Cyber Security Centre.
- The Information Commissioner's Office.

NHS England may also disseminate information to other bodies not listed by using its discretionary dissemination powers.

Data Access Request Service (DARS)

It is not expected that any data collected by the Data Security Centre Services Directions 2020 will be disseminated via DARS.

Publication

Data to be published

NHS England will publish summary and aggregate information for public consumption in a manner and timing that NHS England considers is appropriate. This will consider the need for the information to be easily accessible, the persons who NHS England considers are likely to use the information and the uses to which NHS England considers the information is likely to be put.

Data prohibited from being published

NHS England must not publish any individual data items collected or obtained through the Services, including those outlined in this Specification, unless the SIRO or CISO in consultation with DHSC considers there would be no security risks from doing so, it would be in the public interest to do so and it would otherwise be lawful.

NHS England must not publish any other information collected or obtained through the Services which is considered by the NHS England SIRO or CISO to be a security risk to the health and care sector, or where publication would not be in the public interest, or would not otherwise be lawful. For example, information which must not be published will include but is not limited to:

- Information about organisations who either do or do not have robust data security measures as this may lead to a data security risk for the health and care sector.
- Detailed information about specific incidents and the organisations that were involved in these incidents.
- Information about organisations that have or have not taken up the Services offered in accordance with Data Security Centre Services Directions 2020

System Delivery Function

The existing Cyber Security Operations Centre operates a significant majority of the systems and capabilities required to facilitate the work outlined within these Directions. This has already been funded under the £35m CSOC programme, the £117m local interventions programme, and the £197m Win10 and ATP programme. There is one major procurement left to be completed under the Cyber Security Programme and this is for an Endpoint Defence and Response capability for the server estate.

Change control process

Changes to this Specification will be managed and agreed with the Department of Health and Social Care (on behalf of the Secretary of State) to ensure that any such change is within scope of the Data Security Centre Services Directions 2020.