NHS England

Requirements Specification

Data Security and Protection Toolkit

Version 7

25 September 2024

Information and technology for better health and care

Amendment History:

Version	Date	Amendment History
1.	22 March 2024	First draft.
1.1	20 July 2024	Updated following advice from DAPB
1.2	31 August 2024	Final Review

Approvals:

This document must be approved by the following:

Name	Organisation	Title / Responsibility	Date	Version
Michael Owen	NHS England	Deputy Director, Cyber Operations Senior Responsible Owner	31 July 2024	1.0.
Phil Huggins	DHSC/NHS England	National Chief Information Security Officer for Health & Care Sponsor	31 July 2024	1.0.
Louise Greenrod	DHSC/NHS England	Deputy Director - Data Policy and Digital Oversight Sponsor	31 July 2024	1.0.

Contents

1. Overview

This Requirements Specification is the formal definition of the Data Security and Protection Toolkit (DSPT) Standard.

This document includes the scope of the standard, conformance requirements and timescales for data collection.

If you have any questions about this document, contact details are available from the help menu of the DSPT, under section 2. “Contact Us”.

2. Glossary

Term	Acronym	Definition/ Link
Arm’s Length Body	ALB	An organisation that delivers a public service, is not a Ministerial government department, and which operates to a greater or lesser extent at a distance from ministers e.g. executive agencies such as the Medicines and Healthcare Products Regulatory Agency; special health authorities such as the NHS Business Services Authority
Any Qualified Provider	AQP	AQP services include Musculo-skeletal services for back and neck pain; Adult hearing aid services in the community; Continence services (adults and children); Diagnostic tests closer to home such as some types of imaging, cardiac and respiratory investigations; Wheelchair services; Podiatry services; Venous leg ulcer and wound healing; Primary care psychological therapies (adults).
Care Quality Commission	CQC	CQC Website: Details of inspection regime, including Well-Led key lines of enquiry are available.

Data Access Request Service	DARS	The Data Access Request Service (DARS) can offer clinicians, researchers and commissioners the data required to help improve NHS services.
The Department of Health and Social Care	DHSC	The Department of Health and Social Care (DHSC) supports ministers in leading the nation's health and social care to help people live more independent, healthier lives for longer.
General Data Protection Regulation	GDPR	Regulation on Data Protection
Confidentiality Advisory Group - Health Research Authority	HRA CAG	The Confidentiality Advisory Group (CAG) is an independent body which provides expert advice on the use of confidential patient information. This includes providing advice to us, the Health Research Authority (HRA) for research uses. It also provides advice to the Secretary of State for Health for non-research uses.
Data Security and Protection Toolkit	DSPT	Scope / Purpose as defined in this document
The Information Commissioner's Office	ICO	The ICO exists to empower you through information.
Local Authorities	LA	A county, shire, district, borough or city council responsible for providing public services (including public health teams and adult social care delivery functions) within a defined geographical area.
National Cyber Security Centre	NCSC	The NCSC is the UK's 'technical authority' for cyber incidents. It is part of GCHQ, one of the UK's security services, and was formed in 2016 to provide a unified national response to cyber threats.

National Data Guardian	NDG	The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.
NHS Business Partner	Not Applicable	An organisation that, whilst remaining independent, works closely with NHS organisations and shares common goals for providing high standards of healthcare directly to patients. See here.
NHS Digital	NHS Digital	Historically the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care, now merged with NHS England The Health and Social Care Information Centre was a non-departmental body created by statute, also known as NHS Digital.
NHS England	NHSE	NHS England is an executive non-departmental public body, sponsored by the Department of Health and Social care,
Sensitive Personal Data	N/A	Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation
Secondary Use Organisation	N/A	An organisation that processes patient information for secondary purposes.

3. Related/Supporting Information

The following documents, (available from the relevant links) provide a background to this standard, including the mandate for the DSPT and current policy:

National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016

Government Response "Your Data: Better Security, Better Choice, Better Care" July 2017

Department of Health and Social Care "2017/18 Data security and protection requirements" October 2017

Department of Health and Social Care "Securing cyber resilience in health and care: progress update November 2019"

The cyber security strategy for health and adult social care March 2023 .

4. Definition

The Data Security and Protection Toolkit (DSPT) is an online tool that enables organisations to measure their performance against cyber security and information governance requirements set by the Department of Health and Social Care.

The DSPT was originally developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017 (see section 3).

The DSPT is the successor framework to the Information Governance Toolkit.

5. Background

The DSPT is a Department of Health and Social Care (DHSC) policy delivery vehicle that NHS England is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DHSC policy and presents them in a single standard as a set of requirements. Relevant organisations (as set out in section 7) are required to carry out self-assessments of their compliance against the assertions and evidence items contained within the DSPT.

5.1 Requirements

For NHS Organisations (NHS Trusts, Integrated Care Boards, Commissioning Support Units and Arm's length Bodies) the DSPT allows organisations to measure themselves against the NSCS Cyber Assurance Framework health overlay.

In 2023 our own health and care cyber security strategy committed to adopt the CAF as the principal cyber standard.[1] We believe this will:

- Emphasise **good decision-making over compliance**, with better understanding and ownership of information risks at the local organisation level, where those risks can most effectively be managed.

[1] DHSC 'Cyber security strategy for health and social care: 2023 to 2030'

- Support **a culture of evaluation and improvement**, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes – and expend effort on what works, not what ticks a compliance box.
- Create **opportunities for better practice**, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks.

We have developed a **health and care CAF overlay** that amends some CAF terminology and adds a further 8 outcomes in a custom section on 'using and sharing information appropriately' **to ensure that data protection, confidentiality and other information governance disciplines are fully covered**. The 'health and care CAF' presented in the DSPT will therefore consist of 47 outcomes.

For all other organisations, the DSPT provides a mechanism for organisations to assess themselves against the NDG 10 data security standards, through confirming assertions, and providing supporting evidence (details are provided at Appendix 1 - Assertions and evidence items).

Several assertion statements are identified, relevant to each of the 10 standards. Assertions are positive statements which organisations must review and (where appropriate) confirm.

Each assertion is underpinned by one or more evidence items. These are pieces of information which (where appropriate) should be provided, to evidence assertions. These evidence items can be: a date, a document, yes/no confirmation, a number or text.

Some evidence items are considered a minimum expectation which an organisation must have in place. These are indicated as "mandatory" elements on the DSPT.

The use of "mandatory" functionality aims to ensure attention is focused on those highest priority elements of data security and information governance, whilst providing opportunity for organisations to evidence improvement over time against recommended elements. The recommended elements may become mandatory in future years to improve data security in organisations as data security maturity increases or threats change.

Requirements differ for different organisation types, to reflect data security risk, IT arrangements and digital maturity, see section 8.

Some relevant evidence items will not be required where an organisation uses NHSmail, or has in place an existing relevant standard (Cyber Essentials PLUS, ISO 27001, Public Service Network Information Assurance) where this standard is of an equivalent or higher level than the DSPT.

5.2 Purpose

The purpose of the DSPT is:

(i) For organisations to demonstrate to relevant national and local bodies their compliance with mandated standards for data protection, data security and cyber security;

(ii) To allow organisations to understand the data protection requirements and security risks in relation to their data and essential services, including in comparison to other, similar organisations;

(iii) To enable national and regional bodies to understand data protection requirements and security risk in relation to data and essential services across the health and care system and determine appropriate responses and interventions; and,

(iv) To give the public confidence in how health and care organisations handle and share some of their most sensitive personal data.

Where partial or non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

The ultimate aim is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information. This in turn increases public confidence that 'the NHS' and its partners can be trusted with personal data. This will minimise the number of individuals who 'opt out' of the sharing of their personal identifiable data.

Using the toolkit to perform a self-assessment against the standard and having it independently assured [2], will allow organisations to identify and implement action to address any shortcomings, which in turn will reduce the organisation's risk of a data breach and /or cyber security incident.

For more information on the legal position / mandate, please see section 11.

5.3 Completing the DSPT in support of applications for section 251 approval and requests to the NHS England Data Access Request Service

All bodies (new and existing applicants) that are seeking access to NHS patient information via section 251 NHS Act 2006 applications to the approving body, the Confidentiality Advisory Group - Health Research Authority (HRA CAG), are required to provide Data Security assurances, part of which is submission of a DSPT assessment and to demonstrate a satisfactory level of compliance.

NHS England has taken similar measures in relation to requests for patient data for secondary uses (requests via the Data Access Request Service – DARS). Applicants must provide assurance that good Information Governance practices are being maintained by:

Providing assurance that your organisation meets the NHS England requirements and standards for specified controls (details of which must be provided to DARS directly).

And at least one of the following:

a) Completing a DSPT assessment and meeting a satisfactory level of attainment; or

b) Providing details of certification against the relevant international security standard (ISO); or

c) Demonstrating that other assurances are in place (details of which must be provided to DARS directly).

[2] DSPT Independent Assurance and Audit 2023-24

Any dissemination of patient data for secondary use must also be approved through the DARS process and according to the policies and procedures set out through DARS and supported by Data Sharing Agreement (DSA) and Data Sharing Framework Contract.

NHS England will continue to provide assurances to DARS and HRA CAG.

6. Benefits

The DSPT provides a mechanism for organisations to demonstrate that they can be trusted to maintain the confidentiality and security of personal information. This in turn increases public confidence that ‘the NHS’ and its partners can be trusted with personal information. Organisations can publicise their DSPT assessment to demonstrate they are meeting the NDG Data Security Standards. It is hoped that increased personal confidence will minimise the number of individuals who 'opt out' of the sharing of their personal identifiable data.

The DSPT enables organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

By assessing themselves against the standard and implementing actions to address shortcomings identified though use of the DSPT, organisations should be able to reduce the risk of a data breach and / or cyber security incident.

The General Data Protection Regulation allows the supervising authority (the Information Commissioner’s Office) to levy a maximum fine of £17,500,000 or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year, whichever is greater.

7. Scope

DSPT assessments must be completed and published by:

a) All bodies that process the personal confidential data of citizens who access health services.

b) All bodies that provide adult social care services commissioned via the NHS Standard Contract.

The organisations required to complete a DSPT assessment include, but are not limited to:

c) NHS organisations (Acute Trusts, Ambulance Trusts, Mental Health Trusts, Community Trusts, Care Trusts, (including Foundation Trusts and NHS Community Health Providers) Commissioning Support Units, Integrated Care Boards).

d) Local Authority Adult Social Care.

e) Local Authority Public Health.

f) Primary Care providers (community pharmacies / dispensing appliance contractors, dental practices, eye care services, general practices).

g) DHSC Arm's Length Bodies.

h) Bodies commissioned or otherwise contracted to provide services by any of the above including adult social care providers.

In addition to the NHS mandate above, other organisations are required to provide Data Security and Protection assurances via the DSPT as part of business/service support processes or contractual terms. That is, for these organisations, annual DSPT assessments are required for either or both of two purposes:

i) To provide data security and protection assurances to the Department of Health and Social Care or to NHS commissioners of services;

j) To provide data security and protection assurances to NHS England as part of the terms and conditions of using national systems and services, including the e- Referral Service and NHSmail.

8. Requirements by User Group

The assertions which must be confirmed, and the evidence items which must be provided, vary by organisation type.

Each organisation type is automatically allocated a classification as follows:

Category 1: NHS Trusts, Integrated Care Boards, Commissioning Support Units, Arm's Length Bodies,

Category 1a Organisations that operate critical national infrastructure are subject to a different (stricter) profile due to ministerial expectations for all such organisations across government, originating from the government cyber security strategy [3].

Category 2: IT Suppliers and Organisation designated as Operators of Essential Service under the Network and Information Systems (NIS) Directive.

Category 3: AQP Clinical Services, AQP Non-Clinical Services, Care Home, Charity/Hospice, Company, Dentist (NHS), Dentist (Private), Domiciliary Care Organisation, Local Authority, NHS Business Partner, Optician, Pharmacy, Prison, Researcher/Department, Secondary Use Organisation and University

Category 4: GP Practices

The assertions/outcomes which must be provided by each organisation classification are outlined in Appendix 1 - Assertions and evidence items.

9. Conformance

Relevant organisations MUST publish their assessment via the DSPT annually by 30 June 2024 (full conformance date).

To publish a 'Standards Met" assessment via the DSPT:

[3] Government Cyber Security Strategy: 2022 to 2030

a) NHS organisations (Category 1) must meet the required achievement level across all the outcomes in DSPT taken from the health and care overlay

b) For all other organisations evidence MUST be provided against each mandatory evidence item (as defined in Appendix 1 - Assertions and evidence items).

c) For all other organisations every assertion which includes one or more mandatory evidence item MUST be confirmed.

All Category 1 and 2 organisations are required to commission an annual audit on their DSPT self-assessment submissions.

Organisations registered with the CQC will have data security included in their Well-Led inspection with their DSPT considered as key evidence.

10. Timescales/Plan

10.1 First-time assessments

Organisations carrying out their first assessment should complete this in line with the contract of services they are party to, or as required by the tendering process they are involved in.

For Research Teams or National Registers required to complete a DSPT assessment in support of an application to access patient information held on national systems, held by NHS England or required for processing without consent (for both research and non-research purposes), the DSPT assessment should be completed within given timelines determined by the approval processes concerned (e.g. section 251 approvals by the Health Research Authority Confidentiality Advisory Group).

10.2 Additional assessments

A second or subsequent assessment can be started at any time but in all cases the final publication must be made online by 30 June 2025.

Category 1 NHS organisations (as set out in section 8) are also required to complete an interim assessment during the year – the deadline for the interim submission will be 31 December 2024. This will be publicised by writing to all the organisations covered by the scope of the interim assessments and by communication through the Strategic Information Governance Network, the network of IG leads in large health and care organisations, DSPT Website and Cyber Associates Network.

The work necessary to make improvements or to maintain compliance should be an on-going process and not left until close to the deadline.

Organisations registered with the CQC may have data security included in their Well-Led inspection with their DSPT considered as key evidence.

11. Legal Position / Mandate

11.1 Overview

It is Department of Health and Social Care policy that all organisations which have access to NHS patient information must provide assurances that they are practising good information governance and use the DSPT to evidence this by the publication of annual assessments.

It is also a contractual requirement in the NHS Standard contract(general conditions section 21.2) that relevant providers undertake DSPT assessments on an annual basis: *"The Provider must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider's organisation type."*

It remains Department of Health and Social Care policy that all bodies that process NHS patient information for whatever purpose should provide assurance via the DSPT.

Use of the DSPT is also required as part of the DHSC publication: Data security and protection for health and care organisations October 2017.

Use of the DSPT is required through The Network and Information Systems Regulations 2018: guide for the health sector in England.

NHS England has been directed to undertake this collection by the Department of Health and Social Care through a legal direction.

11.2 Related legislation, policy and good practice

In addition to the above, the standard (and associated guidance) draws together key rules and good practice about how information is handled pertaining to:

- The General Data Protection Regulation May 2018.
- The Data Protection Act 2018.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review' (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2 Review
- Lessons learned review of the WannaCry Ransomware Cyber Attack (NHS England February 2018)
- Department of Health and Social Care publication: "Securing cyber resilience in health and care: progress update" November 2019

- A cyber resilient health and adult social care system in England: cyber security strategy to 2030.

12. Data Flow

The DSPT is available to all users via the internet. More information on data flow is available.

13. Data Set

The data captured by the system comprises:

a) Dates

b) Text (including contact details, narrative)

c) Yes/No confirmations

d) KPIs (e.g. values of fines, number of incidents, percentage of suppliers with relevant contract clauses)

e) Documents (e.g. policies, forms, action plans, links to documents or websites)

f) Achievement levels against outcomes

g) Supporting statements explaining how an organisation is meeting an achievement level.

Details of the data items are provided in Appendix 1 - Assertions and evidence items .
Details of timescales are provided in section 10.

14. Useful Information

A list of URLs and links used in this document.

DSPT Contact Us

https://www.dsptoolkit.nhs.uk/Home/Contact

Care Quality Commission

https://www.cqc.org.uk/about-us

Data Access Request Service

https://digital.nhs.uk/services/data-access-request-service-dars

Department of Health and Social Care

https://www.gov.uk/government/organisations/department-of-health-and-social-care/about

General Data Protection Regulation
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Confidentiality Advisory Group - Health Research Authority

https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/

The Information Commissioner's Office

https://ico.org.uk/

National Data Guardian

https://www.gov.uk/government/organisations/national-data-guardian

NHS England

https://www.england.nhs.uk/

National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016

https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

Government Response "Your Data: Better Security, Better Choice, Better Care" July 2017

https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

Department of Health and Social Care "2017/18 Data security and protection for health and care organisations" October 2017.

https://www.gov.uk/government/publications/data-security-and-protection-for-health-and-care-organisations

Department of Health and Social Care Securing cyber resilience in health and care: progress update November 2019

https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-progress-update-2019

NHS Standard contract

https://www.england.nhs.uk/nhs-standard-contract/

DSPT privacy information

https://www.dsptoolkit.nhs.uk/Home/Privacy

Appendix 1 - Assertions and evidence items

https://www.dsptoolkit.nhs.uk/News/131