Implementation Guide

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	1.1
Phil Huggins	DHSC/NHS England	National Chief Information Security Officer for Health & Care Sponsor	31 July 2024	1.1
Louise Greenrod	DHSC/NHS England	Deputy Director - Data Policy and Digital Oversight Sponsor	31 July 2024	1.1

Contents

1. Overview

This document provides guidance to all impacted users on how to implement and use the Data Security and Protection Toolkit (DSPT) information standard.

2. Related/Supporting Information

The following documents provide background to this standard, including the mandate for the DSPT and current policy and can be accessed through the following links:

- 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 for health and care organisations" 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.

Guidance materials for users are available on the help pages of the DSPT:

3. Definition

The 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 has been 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.

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

4. 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.

Furthermore, it is recommended that all other social care providers also complete a DSPT.

The organisations that are required to complete the DSPT 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.

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:

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

b) 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

5. 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 [1].

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

[1] Government Cyber Security Strategy: 2022 to 2030

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 Requirements Specification **Error! Reference source not found.**.

6. Timescales/Plan

6.1 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).

6.2 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 (NHS Trusts, Arm's Length Bodies, Integrated Care Boards, Commissioning Support Units 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.

7. Helpdesk

Users should raise all incidents and support requests with the DSPT helpdesk. Support requests can be raised by telephone (9.00 – 17.00 on weekdays) or by email. Contact details are available from the help menu of the DSPT, under section 2 "Contact Us".

Target service levels for the helpdesk (and service availability) are summarised below:

Description	Target
Total supported service availability (excluding planned downtime)	98%
Period of planned downtime	Maximum of 10 working days per annum
Restoration of full production service to failover infrastructure	Within 4 hours

All incidents are dealt with in order of priority allocation, with 1 being the highest order of priority.

Incident categorisations, and target resolution timescales are as detailed in the table below:

Service Impact (see following table)	Overall % Target	Priority Derived	Response Within	Resolution Within
High	99%	1	2 hours	3 working days
Significant	95%	2	4 hours	6 working days
Medium	95%	3	No target	10 working days
Low / None	95%	4	No target	As agreed

An incident or support request may pass from 1st to 2nd to 3rd line support teams within these timescales. From a user's perspective it is one incident or support request raised and dealt with in the timescales outlined.

8. Guidance by user group

8.1 Overview

The DSPT is designed to enable most users to be able to complete and publish an assessment without reference to detailed guidance documentation.

Where required, evidence items on the DSPT are accompanied with concise guidance / prompts to aid organisations in providing a suitable response. The evidence items (and concise guidance) vary depending on the classification of the organisation (see Requirements Specification section 8).

Additional guidance documents have been provided to support organisations which require additional clarity on the assessment process, or on the implementation of good Data Security, Cyber Security and Information Governance.

8.2 Agile development

In accordance with requirements of the Government Digital Service, the DSPT is being developed utilising an agile methodology informed by ongoing user research. New functionality, and refinements to the existing interface, are being developed on a continuous basis, with the DSPT functionality updated (typically) on a fortnightly basis, but the assertion wording being stable to ensure organisations are meeting an equal standard.

These agile principles will be applied to guidance documentation, which will be subject to continuous review and refinement to reflect user feedback and/or changes to the functionality of the system.

8.3 Guidance documentation

Guidance materials are available via the DSPT Help pages.

The guidance includes (but is not limited to):

c) Introductory guidance

d) “About the Data Security and Protection Toolkit “

e) Data Security Standard “Big Picture Guides”

f) “Organisation Type” guidance

g) Frequently asked questions documentation

h) Guidance documents for large NHS Organisations completing a 24-25 Data Security and Protection Toolkit. These have been developed in conjunction with NHS Organisations to ensure they provide the help and support required.

i) In addition, a change log and pipeline of future development is available on the DSPT.

j)

Additional guidance materials may be developed where user research identifies a need. Digital Social Care and Pharmaceutical Services Negotiating Committee (PSNC) have developed information to assist the social care and pharmacy sectors:

Pharmaceutical Services Negotiating Committee Guidance

Digital Social Care Guidance

8.4 Useful Information

A list of URLs and links used in this document.

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

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

https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030

Help pages of the DSPT

https://www.dsptoolkit.nhs.uk/Help/

DSPT Contact Us

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

Pipeline of future development available on the DSPT

https://www.dsptoolkit.nhs.uk/News/release-notes

Pharmaceutical Services Negotiating Committee Guidance

https://psnc.org.uk/digital-and-technology/data-security/data-security-and-protection-toolkit/

Digital Social Care Guidance

https://www.digitalcarehub.co.uk/dspt/