Change 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	1.2.
Phil Huggins	NHS England	National Chief Information Security Officer for Health & Care Sponsor	31 July 2024	1.2.
Louise Greenrod	DHSC/NHS England	Deputy Director - Data Policy and Digital Oversight Sponsor	31 July 2024	1.2

Contents

1

1. Overview 4

2. Definition 4

3. Guidance by user group 4

4. Statement of all changes to the published Requirements Specification 5

4.1 DSPT version 7 – overview of changes 5

4.2 DSPT changes – rationale and examples 5

4.3 Annual review 6

4.4 DSPT version 5 and 6 comparison 7

5. Change control during 2024-25 7

6. Useful Information 7

Appendix 1 – DSPT 2023-24 (version 6) to 2024-25 (version 7) mapping 8

Appendix 2 DSPT 2024-25 for Category 1 and 1a Version 6 to Version 7 mapping 8

1. Overview

The proposed changes to the standard will see NHS organisations (NHS Trusts, Integrated Care Boards, Commissioning Support Units and Arm's length Bodies utilise the National Cyber Security Centre (NCSC) Cyber Assessment framework introduced into the Data Security and Protection Toolkit (DSPT) in line with the Cyber Strategy for health and care [1] For other organisations the changes will improve clarity of language and update the requirements to support cyber resilience.

This will be a change for NHS organisations.

This Change Specification outlines the key differences between the DSPT version 6 (2023-24) and the updated DSPT version 7 (2024-25).

This document should be read in conjunction with the DSPT Requirements Specification (specifically Appendix 1 – Assertions and Evidence items) and Implementation Guidance.

2. 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 Toolkit 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. It is being developed further following the publication of the DHSC 'Cyber security strategy for health and social care: 2023 to 2030'

The Data Security and Protection Toolkit is the successor framework to the Information Governance Toolkit.

3. Guidance by user group

In accordance with the requirements of the Government Digital Service, the design and content of the DSPT have been developed to ensure that the system is easy to use. The solution is designed to enable most users to be able to complete and publish an assessment without reference to detailed guidance documentation. The system has been developed in consultation with users and stakeholders.

Guidance materials are made available via the DSPT Help pages and via the tooltips associated with evidence items. Guidance which is suitable for all sectors has been included, tested with users and updated following consultation. For the two largest sectors (Adult social care and Pharmacy), specific guidance has been developed to further support these sectors. This has been co-developed with the sector.

For more information, please refer to the DSPT Implementation Guidance documentation.

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

4. Statement of all changes to the published Requirements Specification

4.1 DSPT version 7 – overview of changes

The DSPT Standard is reviewed annually. The proposed 2024-25, version 7 standard sees a reduction in the total number of responses required for NHS organisations, Key IT suppliers and Independent providers who are designated operators of essential services under Network and Information Systems directive (NIS)[2] and is unchanged for all other sectors.

A summary of the changes in this release::

- NHS organisations (NHS Trusts, Integrated Care Boards, Commissioning Support Units and Arm's length Bodies utilise the NCSC Cyber Assessment framework introduced into the DSPT in line with the Cyber Strategy for health and care [3]
- Rationalise evidence items where there is overlap between evidence items.
- Reflect feedback from stakeholders particularly:
  Update the requirements for Key IT Suppliers and Independent Providers who have been designated Operators of Essential Services to ensure they are fully applicable to them.
  Update requirements for smaller organisations to align with Information Commissioners Office (ICO) and NCSC guidance from small businesses. Most significantly adding a requirement for multifactor authentication for remote access as a key lesson from recent cyber security incidents.

4.2 DSPT changes – rationale and examples

NHS organisations (NHS Trusts, Integrated Care Boards, Commissioning Support Units and Arm's length Bodies utilise the NCSC Cyber Assessment framework introduced into the DSPT in line with the Cyber strategy for health and care, this will:

4.2.1 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 with increased flexibility about how they are managed.

4.2.2 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.

4.2.3 Create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks.

[2] The Network and Information Systems Regulations 2018: guide for the healthhttps://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-health-sector-guide/the-network-and-information-systems-regulations-2018-guide-for-the-health-sector-in-england sector in England
[3] DHSC 'Cyber security strategy for health and social care: 2023 to 2030'

Rationalise evidence items where there is overlap between evidence items.

4.2.4 Each year evidence items are reviewed alongside feedback from users to rationalise evidence items.

4.2.5 Two evidence items have removed for CAT3 organisations due to overlap with other evidence items and not providing additional assurance beyond what is given in other evidence items.

Reflect feedback from stakeholders particularly to update the requirements for Key IT Suppliers and Independent Providers who have been designated Operators of Essential Services to ensure they are fully applicable to them.

4.2.6 One evidence item has been removed for IT Suppliers and independent providers who have been designated Operators of Essential Services which is related to clinical coding, which is not a requirement for these organisations.

Update requirements for smaller organisations to align with DHSC Joint Cyber Unit (JCU) advice, ICO and NCSC guidance from small businesses. Most significantly adding a requirement for multifactor authentication for remote access as a key lesson from recent cyber security incidents.

4.2.7 Two evidence items have been added for CAT3 organisations to align with updated guidance from the ICO and the NCSC covering Firewalls and Multi-factor authentication.

4.3 Annual review

4.3.1 The proposed updates to the previous DSPT 2022-23 standard have led to a small reduction in total number of evidence items in Category 1 and Category 3. Comparative breakdowns of both the total number of evidence items and total number of mandatory evidence items are provided in the tables below:

	Category 1 organisations	Category 2 organisations	Category 3 organisations	Category 4 organisations
Total number of evidence items 2023-24 v6	128	131	77	39
Total Number of evidence items/outcomes 2024-25 v7	47	128	77	40

Figure 1

	Category 1 organisations	Category 2 organisations	Category 3 organisations	Category 4 organisations
Total number of mandatory evidence items 2023-24 v6	109	109	42	28
Total number of mandatory evidence items 2024-25 v7	47	108	43	29

Figure 2

4.4 DSPT version 6 and 7 comparison

Appendix 1 provides the DSPT 2024-25 (version 7) requirements together with details of changes and mapping when compared to DSPT 2023-24 (version 6), including those evidence items which have been removed.

5. Change control during 2024-25

System refinements and new functionality will be deployed throughout 2024-25. Details of these changes will be set out within the "System changes and release notes" page on the DSPT: https://www.dsptoolkit.nhs.uk/News/release-notes . Material changes to the wording in the standards themselves will only be made in exceptional circumstances, such as where new legislation amends the requirement. This would be communicated to the users via email to those directly affected and set out within the "Standard changes and release notes" page on the DSPT help page.

6. 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

Help pages of the DSPT

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

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

Pipeline of future development available on the DSPT / System changes and release notes"

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

Appendix 1 – DSPT 2023-24 (version 6) to 2024-25 (version 7) mapping

Please refer to separate file:

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

Appendix 2 DSPT 2024-25 for Category 1 and 1a Version 6 to Version 7 mapping

Please refer to separate file:

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