NHS England

DSP Toolkit update

September 2024

Presented by:
John Hodson

Data Security and Protection Toolkit

What is it?

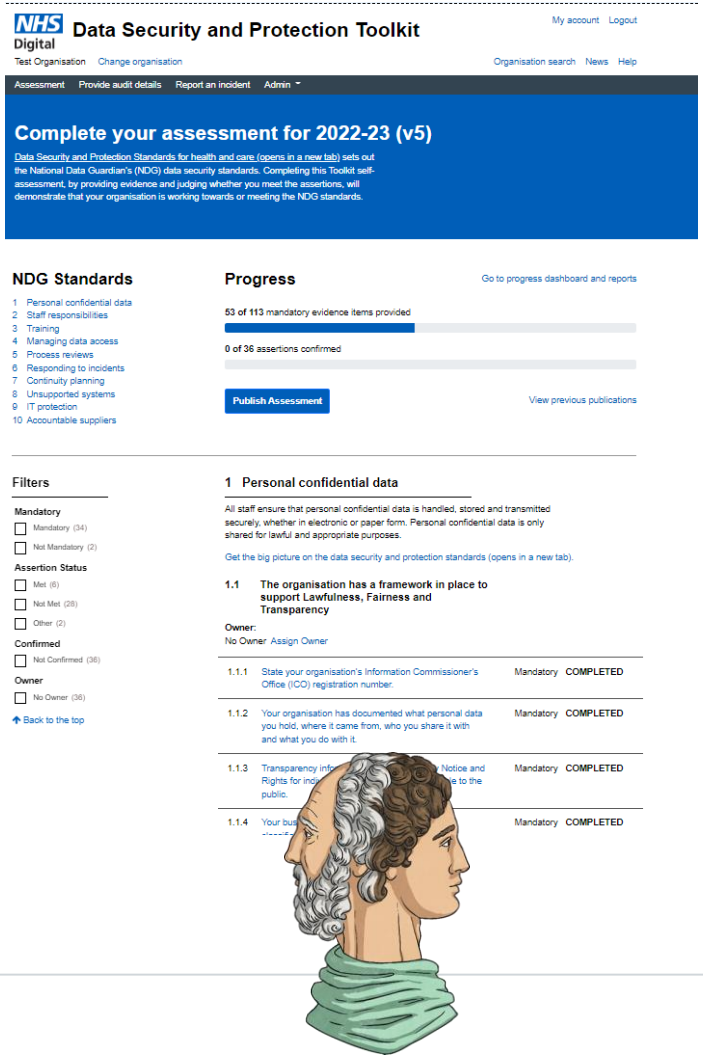
On line Self-Assessment

External assurance

Checklist (DP/Cyber Poverty)

Gateway to systems

Mix of measures (descriptions/outcomes/ checks)



Sector baseline standard

High quality data source

DHSC assurance

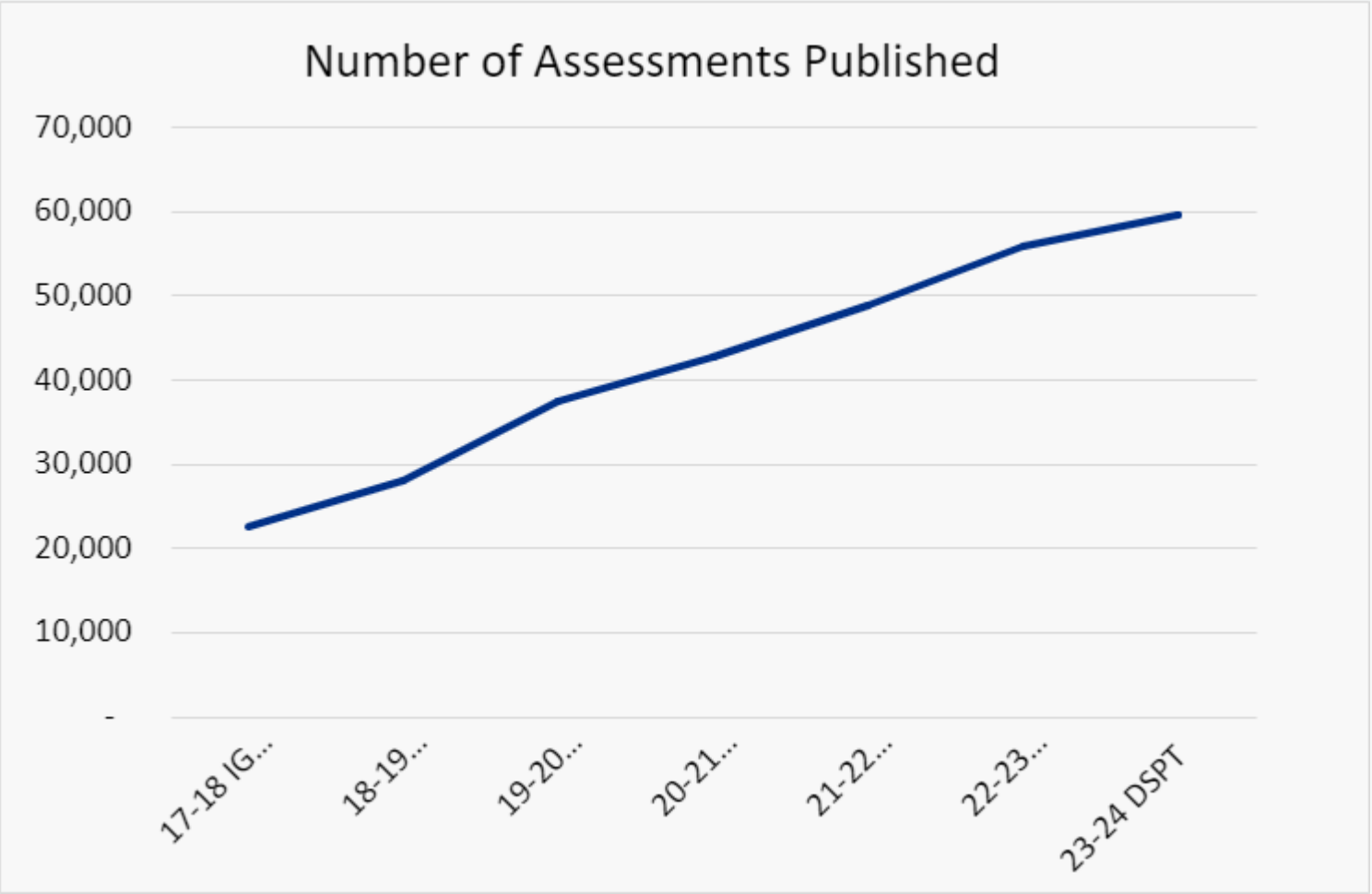
Threat horizon scanning

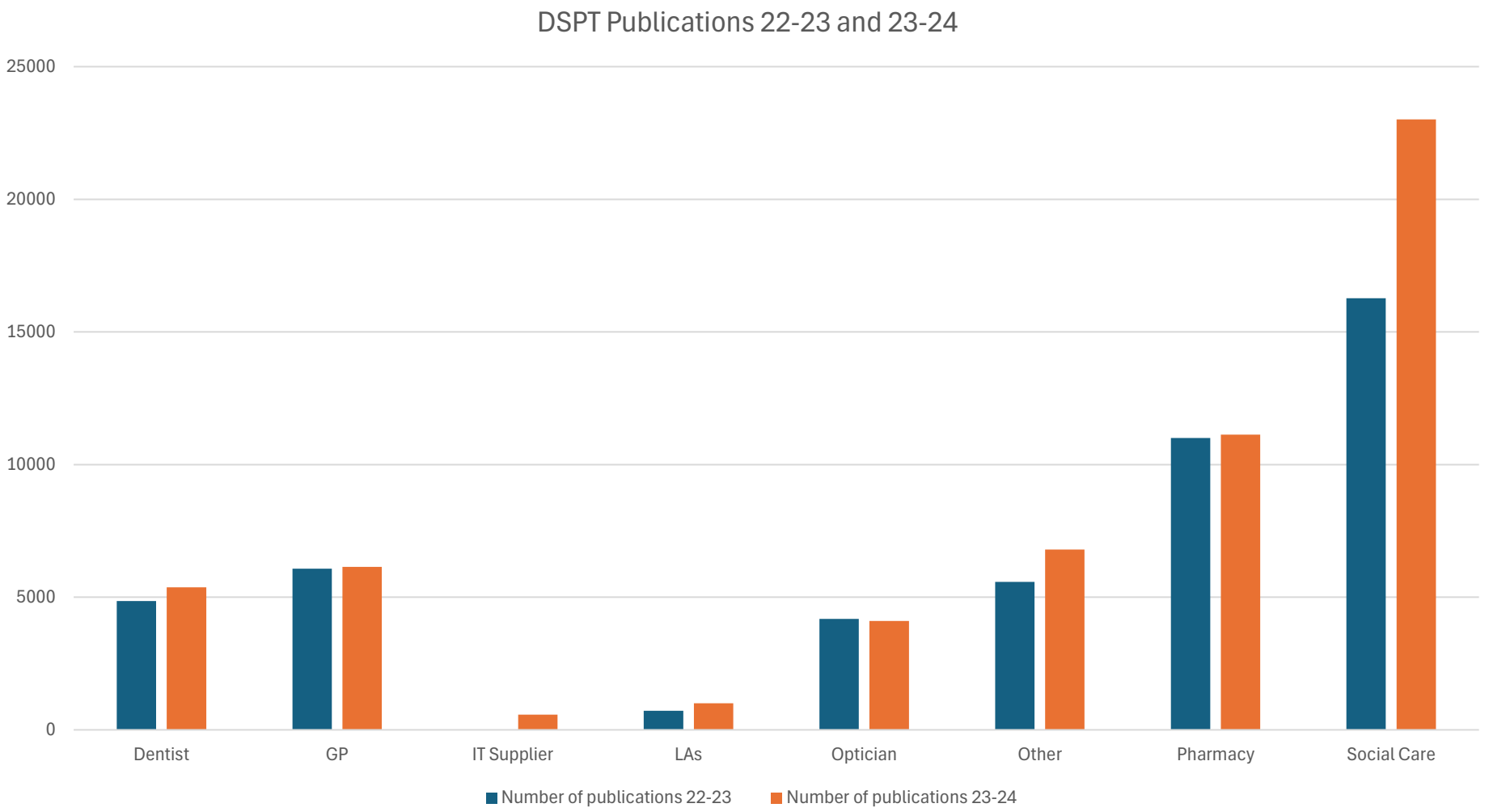
Raising maturity (achievable at a stretch)

23-24 Results

Nearly 60,000 publication for 23-24

Record number of DSPT publications





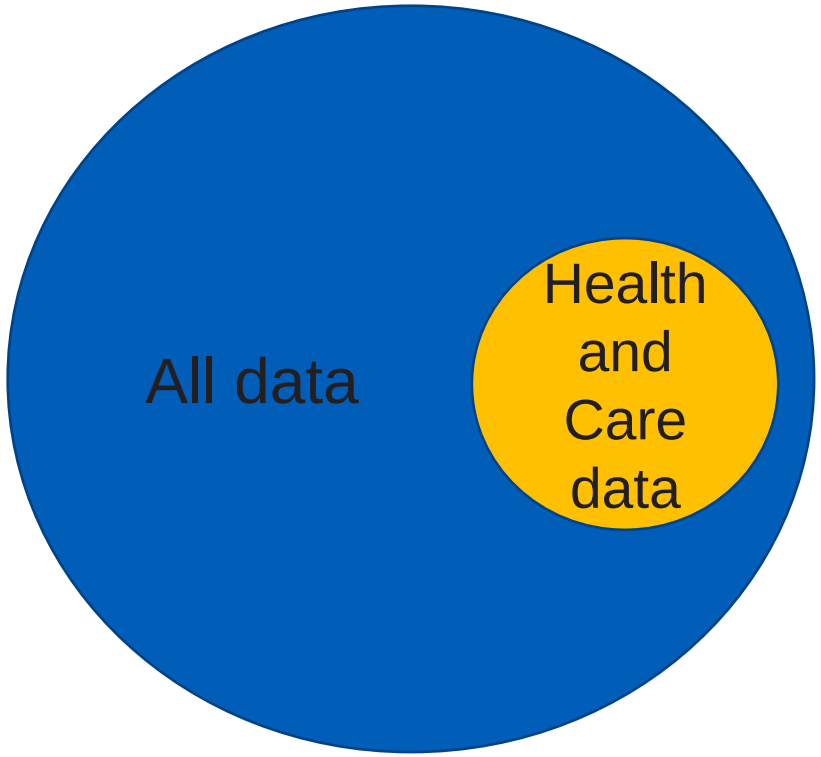
	Number of publications	
Sector	22-23	23-24
Dentist	4854	5373
GP	6077	6146
IT Supplier	0	574
LAs	717	999
Optician	4180	4108
Other	5574	6796
Pharmacy	10998	11127
Social Care	16272	23015

Data as of 15 August 2024. Social care data re-baselined Aug 2023 to match Better Security Better Care number of ASC figures due to scoping assumptions.
Local Authority figures includes owned care homes.

Scope

DSP Toolkit Scope

- DPST Toolkit Standard only Covers health and care data.
- Other areas of the organisation do not need to be included
- This applies to all evidence items e.g. Training, asset register etc.,



DSPT 24-25

Key facts

24-25 launched

Accesses through DSPT

Deadline 30 June 2025

Spreadsheet version available

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

Minor changes overall

8 Tooltip changes

1 new evidence item

1 evidence item merged

Exemptions

NHS Mail

ISO27001

CE+

Standards Exceeded

Standards met plus CE+ certification in the last twelve months prior to date of publication

Changes

Evidence item 1.1.2

Note added in tooltip to clarify the scope is health and care.

Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	You should document your information assets and flows relevant to or supporting health and care services in a combined register, which should have been reviewed and approved by relevant group/person with delegated responsibility since 1st July 2023. You may previously have captured these in separate records of processing activities (ROPA) and information asset and data flows registers (IAR). Details of who conducted the register review and approval, along with when it occurred, should be submitted in the comment box. [Further information on what should be included is available](https://www.dsptoolkit.nhs.uk/Help/88).

Evidence item 1.1.3

Note added to tooltip about transparency

Privacy information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.	You must display transparency information so that people understand how their data is used and shared. If possible, provide a web link or another publicly available document, and detail how printed materials are made available to people if relevant (for example, patient information leaflets provided to patients upon admission to the service). [Guidance on privacy notices is available at the Information Commissioner's Office website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/).

Evidence item 1.1.6

Note added in tooltip to clarify the scope is health and care.

Your organisation has reviewed how it asks for and records consent to share personal data.	Health and/or care organisations may require patient consent under data protection legislation for activities such as patient mailing lists. More commonly, patient consent is required under the common law duty of confidentiality. This would apply in situations when a patient's data is used in ways they would not reasonably expect, for example, when used for research purposes. Consent is also required when sharing confidential patient information with a third party, such as a carer or family member. Please provide details of all your organisation's activities in the comments. Consent should be covered in general data protection and confidentiality policies or a separate consent policy in line with [Information Commissioner's Office guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/). You should ensure that you clearly differentiate between consent under data protection legislation and consent under the common law duty of confidentiality. If an organisation is not using consent to process health and/or care data, it should tick Yes and state in the comments that the organisation does not use consent to process health and/or care data.

Evidence item 1.2.4

Note added in tooltip to explain how organisations not using consent to process health and/or care data should respond to this requirement.

Your organisation is compliant with the national data opt-out policy.	Please provide a link to your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) in the comments box, which might be within a privacy notice or a published data release register. If your organisation is not in scope for the National Data Opt Out, then tick and write "Not applicable" in the comments box.

Evidence item 3.1.1

Note added in tooltip to clarify the scope is health and care.

Training and awareness activities form part of organisational mandatory training requirements, with a training and awareness needs analysis (covering all staff roles) that is formally endorsed and resourced by senior leadership.	You should upload your Training Needs Analysis (TNA) document including details of how you have determined the appropriate training and awareness needs of different staff groups and who has endorsed the document. The TNA should show the details of the different teaching and communication techniques in use, each showing the intended audience. You should also upload a document setting out details of how you make information available in appropriate ways for all staff groups, e.g. intranet pages, posters, briefings at staff meetings etc. This can form part of the overall TNA document. Support and guidance on TNA is available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-3---staff-training/training-needs-analysis-and-delivery-3.1.1-to-3.1.3 If your organisation is an IT supplier, this should cover staff involved in services provided in the role of supplier to health and care organisations.

Evidence item 3.1.2

Note added in tooltip to clarify the scope is health and care.

Your organisation's defined training and awareness activities are implemented for and followed by all staff.	You should provide details of: Initial and refresher activities and expected intervals, for all staff roles, and how you ensure all staff receive them. The proportion of staff completing their role-appropriate training or awareness in the last interval period. Support and guidance is available at:https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-3---staff-training/training-needs-analysis-and-delivery-3.1.1-to-3.1.3. If your organisation is an IT supplier, this should be followed by all staff involved in services provided in the role of supplier to health and care organisations.

Evidence item 4.2.1

Note added in tooltip to clarify the scope is health and care.

When was the last audit of user accounts with access to the organisation's systems held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. E.g. Request and compare the organisation's leavers list from HR, to its Active Directory (AD) user list to determine if there are any leavers that still have access to the organisation's systems. Record the date when the last user audit was held. This should be completed annually as a minimum. If your organisation is an IT supplier, this is all staff accounts involved in services provided in the role of supplier to health and care organisations.

Evidence item 4.2.2

Note added in tooltip to clarify the scope is health and care.

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals. The summary should also include details of whether remediating actions have been implemented. If your organisation is an IT supplier, this is all incidents involved in services provided in the role of supplier to health and care organisations.

Evidence item 4.3.1

Note added in tooltip to clarify the scope is health and care.

All system administrators have signed an agreement which holds them accountable to the highest standards of use.	With great power comes great responsibility and all administrators should attest to that responsibility by being signatory to a agreement affirming the highest standard of use. Your organisation holds documented evidence that systems administrators have been made aware of their increased responsibilities and have signed an enhanced acceptable use policy statement If your organisation is an IT supplier, this is all systems involved in services provided in the role of supplier to health and care organisations.

Evidence item 6.1.1

Note added in tooltip to clarify the scope is health and care.

Data security and protection incidents are reported appropriately and by a full range of staff groups.	You should confirm that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool for health and care incidents or for IT suppliers, this should cover incidents in services provided in the role of supplier to health and care organisations. You should include in the comments the number of incidents and near misses reported per staff group in your organisation, as a proportion of the number of people in each group.

Evidence item 6.3.2

Note added in tooltip to clarify requirement if not applicable.

The organisation uses the ‘Respond to an NHS cyber alert’ service to acknowledge each high severity cyber alert within 48 hours of issue, and additionally to report within 14 days of issue either its implementation and any outstanding plans to follow the advice within the alert, or the approved decision not to do so.	Your response [should cover 'high severity' cyber alerts](https://digital.nhs.uk/services/respond-to-an-nhs-cyber-alert) issued over the last 12 months. If your organisation is an IT supplier, then tick and write "Not applicable" in the comments box.

Evidence item 7.1.1

Note added to include services supported.

Your organisation understands the health and care services it provides or supports.	Provide one or more documents which identify: i. What your organisation's key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service. Documentation should have been reviewed in the last twelve months.

Evidence item 9.3.8

Note added in tooltip to clarify requirement if not applicable.

The organisation maintains a register of medical devices connected to its network.	The register should be uploaded and include Vendor, maintenance arrangements, any network segmentation is in place and whether network access is given to supplier/maintainer.
	If your organisation does not operate any medical devices connected to the network, then select Enter text describing the document's location and write "Not applicable" in the text box.

Evidence item 4.5.3

New requirement for IT Suppliers

For IT Suppliers Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as approved by your board or equivalent senior management. For Independent providers who are Operators of Essential Servies Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.	For IT Suppliers You should particularly consider all systems that can be accessed from the internet – such as email and any cloud-based or online systems – and either ensure that all user accounts are protected with MFA, or detail any exceptions in the text box response. For Independent providers who are Operators of Essential Servies The national MFA policy requires that organisations must enforce MFA on all remote access, and on all privileged accounts on external systems, and should enforce MFA on privileged accounts on internal systems. If you rely on any of the specific exceptions allowed by the policy, you must provide (within your response to this assertion) a summary of your internal approvals and your plans to minimise or eliminate those exceptions. Full detail is given in the [policy]https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy) and [explanatory guidance](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy/guide-to-multi-factor-authentication-policy).

4.5.3 Multi Factor Authentication IT Suppliers

Scoping

- All = Health and care systems
- Remote access accessed from the internet
- Privileged users

Delivery

- Check if systems are for health and care
- Allow remote access and privileged accounts
- Need to check if system is protected by MFA and document it
- Many orgs added extra field to Information asset register

Exemptions

- Recorded for each system
- Approved by board or senior management

4.5.3 Multi Factor Authentication – Independent Providers

Scoping

- All = Health and care systems
- Remote access accessed from the internet
- Privileged users

Delivery

- Check if systems are for health and care
- Allow remote access
- Need to check if system is protected by MFA and document it
- Many orgs added extra field to Information asset register

Exemptions

- Recorded for each system
- Approved by board or senior management

Audit

Audit

Audit Guidance and scope published on DSPT

Same scope as last year

Find an auditor

Set up Auditors with Audit access to DSPT

Work with auditor to agree audit report

Auditors to upload details to DSPT

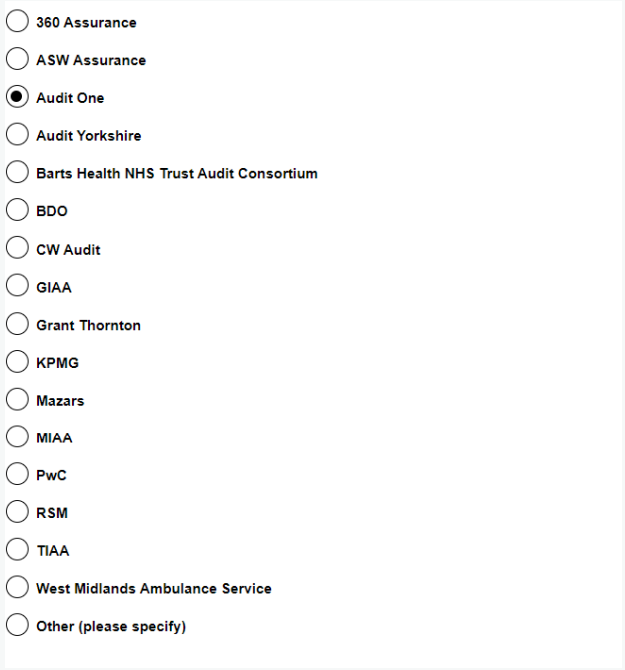
New publication not required

If your audit is not final on 30th June, upload a draft report and then update after the deadline

Who can provide the audit?

The DSPT does not maintain a list of approved auditors.

List of organisations who completed audit last year



There is also a Framework available to purchase from (but it is not mandatory):

https://www.sbs.nhs.uk/article/16541/Internal-and-External-Audit-Counter-Fraud-and-Financial-Assurance-Services

What will the Audit Cover for 23-24

13 assertions:

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency (Auditors are not required to include 1.1.7 and 1.1.8 in the audit scope)
2.2 Staff contracts set out responsibilities for data security
3.1 Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness
3.2 Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents
4.5 You ensure your passwords are suitable for the information you are protecting
5.1 Process reviews are held at least once per year where data security is put at risk and following DS incidents
6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway
7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services
8.2 Unsupported software and hardware is categorised and documented, and data security risks are identified and managed
9.2 A penetration test has been scoped and undertaken
9.5 You securely configure the network and information systems that support the delivery of essential services
9.6 The organisation is protected by a well-managed firewall
10.2 Basic due diligence has been undertaken against each supplier that handles personal information
https://www.dsptoolkit.nhs.uk/News/auditnews

Existing certifications and audits

The scope applies to mandatory evidence items only and with the highlighted evidence items out of scope. Evidence items which are covered by an exemption for CE+ and/or ISO27001 will not require further auditing, once it is confirmed that the scope of the certification covers all the health and care data being processed.

Existing certifications and audits

If you have ISO 27001 or Cyber Essential + certification covering the scope of the DSPT (health and care data) you not have to audit all of the evidence items

Check the DSPT Spreadsheet at https://www.dsptoolkit.nhs.uk/News/131

CE+ evidence items exempt

4.5.1, 4.5.2, 6.2.1, 6.2.3, 6.2.4, 6.2.5, 9.2.1, 9.2.3, 9.5.5, 9.5.6, 9.5.7, 9.5.8, 9.5.9, 9.6.1, 9.6.2, 9.6.3, 9.6.4, 9.6.5, 9.6.6,

IS27001 evidence items exempt

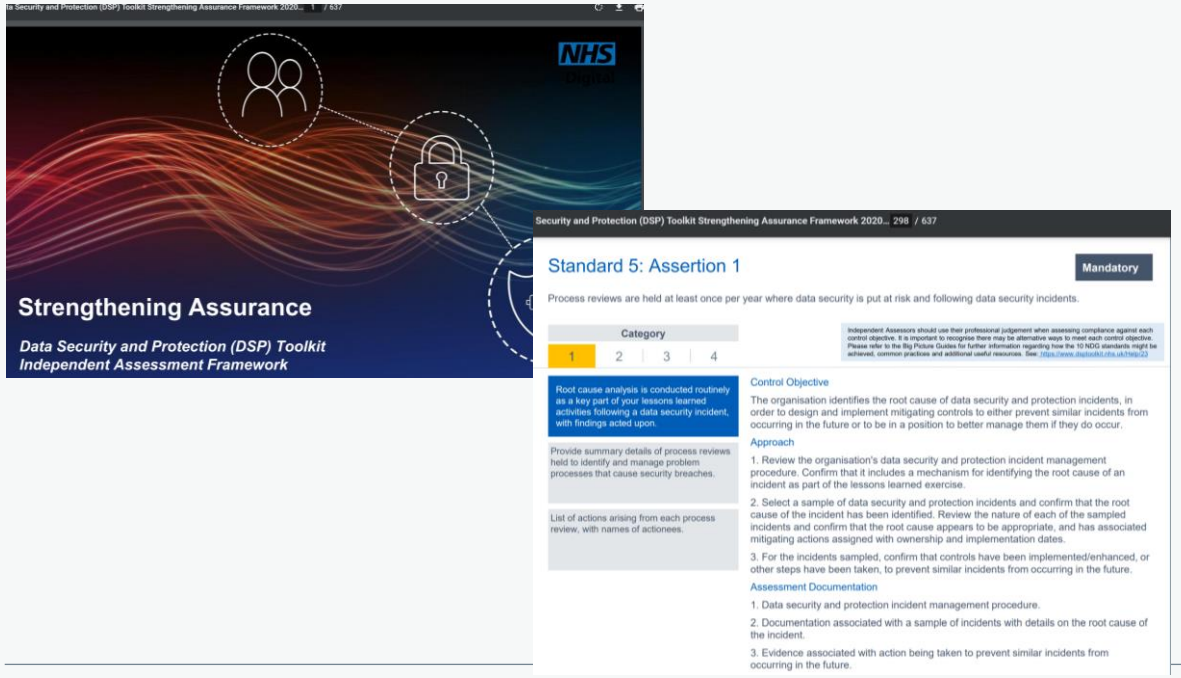
2.2.1, 3.1.1, 4.5.1, 5.1.1, 6.2.1, 7.1.2, 7.1.3, 9.6.1, 10.2.3, 10.2.4,

Resources to help on Audit

Audit Guides

https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides

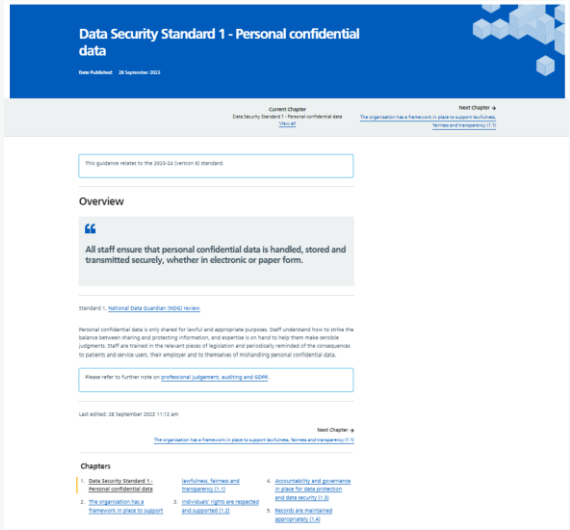
Useful as set out the requirement in a ISO 27001 style with control objective and documentation.



Big Picture Guides

https://www.dsptoolkit.nhs.uk/Help/big-picture-guides

Give background to the requirement and talk more broadly about the subject area with links to wider reading



Improvement Plans

Improvement plans

All organisations at Approaching Standards required to provide an update by end of September 2024

Update to Template plan

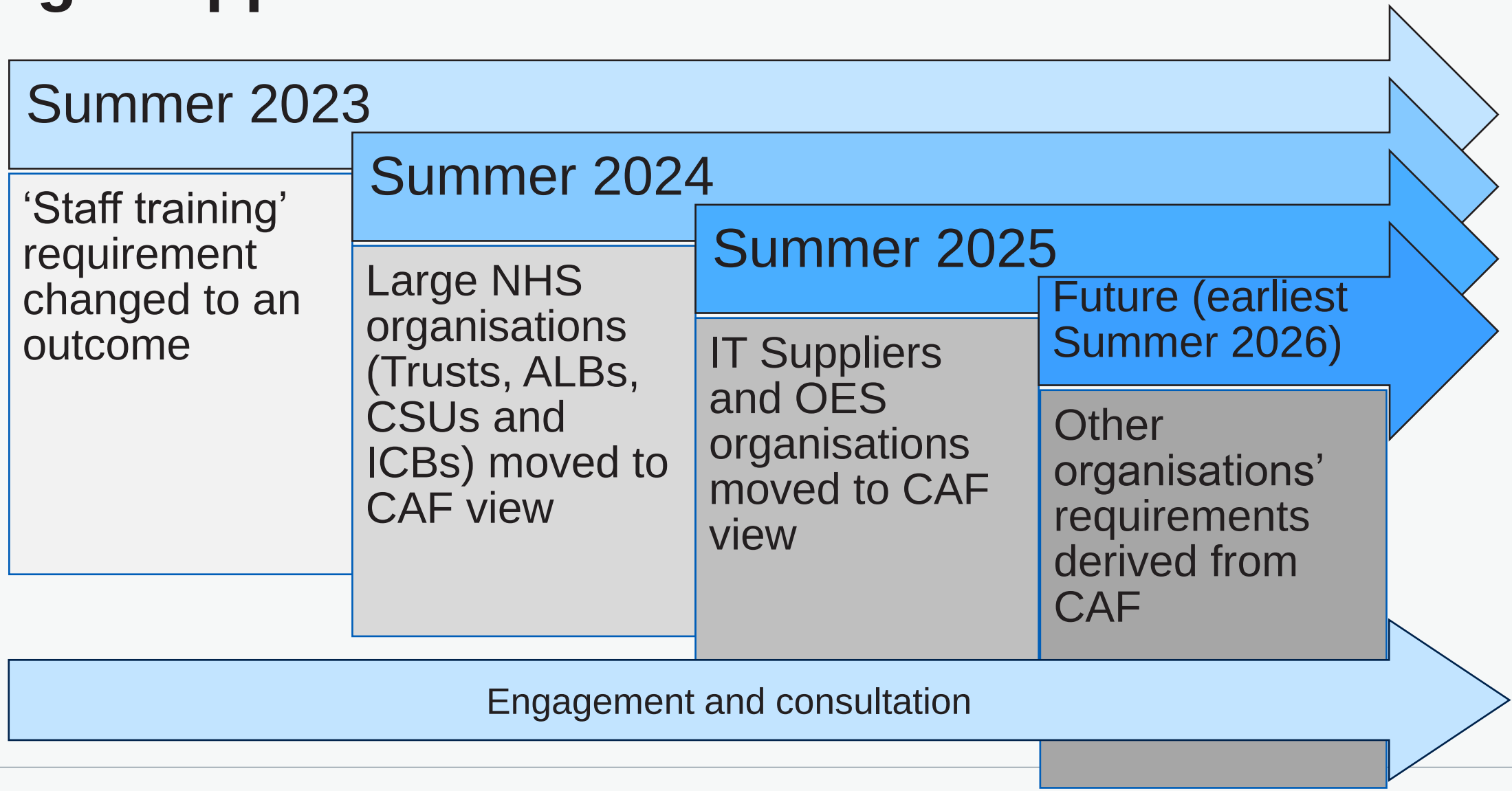
Does not require a publication

Emailed to cybersecurity@nhs.net

Will be reviewed for progress and shared with NHS England and DHSC

25-26 DSPT

Staged approach for DSPT



Help and Support

Resources to help

Overview

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

Videos

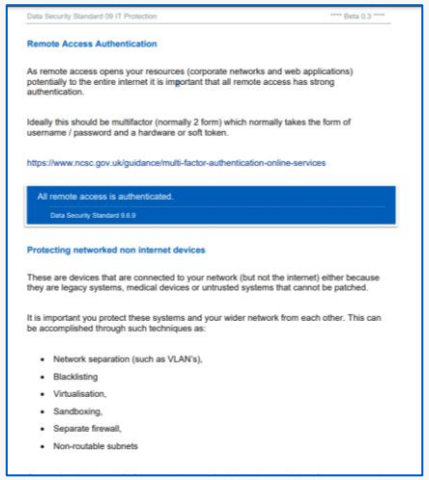
https://www.digitalsocialcare.co.uk/latest-guidance/video-guides-how-to-complete-the-data-security-protection-toolkit/

Overview of what's coming in 25-26
https://www.dsptoolkit.nhs.uk/News/Webinar-Slides

Big Picture Guides

https://www.dsptoolkit.nhs.uk/Help/big-picture-guides

Give background to the requirement and talk more broadly about the subject area with links to wider reading



Data Security and Protection Toolkit

NHS Digital

2021-22 (version 4)

Test Small Organisation

2 Gelder Road, Leeds, West Yorkshire, England, LS12 3UF

Standards Met

Date of publication: **9 July 2022** **(valid to: 30 June 2023)**

This organisation has completed a Data Security and Protection Toolkit self-assessment to demonstrate it is practising good data security and that personal information is handled correctly.

www.dsptoolkit.nhs.uk/

Any Questions

NHS Digital

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk