

DSP Toolkit – Integrated Care Boards

What's new for 22-23

January 2023 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)

NHS Digital Data Security and Protection Toolkit

My account Logout

Test Organisation Change organisation Organisation search News Help

Assessment Provide audit details Report an incident Admin

Complete your assessment for 2022-23 (v5)

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

- 1 Personal confidential data
- 2 Staff responsibilities
- 3 Training
- 4 Managing data access
- 5 Process reviews
- 6 Responding to incidents
- 7 Continuity planning
- 8 Unsupported systems
- 9 IT protection
- 10 Accountable suppliers

Progress

Go to progress dashboard and reports

53 of 113 mandatory evidence items provided

0 of 36 assertions confirmed

[Publish Assessment](#) [View previous publications](#)

Filters

Mandatory

- Mandatory (34)
- Not Mandatory (2)

Assertion Status

- Met (6)
- Not Met (28)
- Other (2)

Confirmed

- Not Confirmed (36)

Owner

- No Owner (36)

[Back to the top](#)

1 Personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

[Get the big picture on the data security and protection standards \(opens in a new tab\).](#)

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency

Owner:
No Owner [Assign Owner](#)

1.1.1 State your organisation's Information Commissioner's Office (ICO) registration number.	Mandatory	COMPLETED
1.1.2 Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Mandatory	COMPLETED
1.1.3 Transparency information: Notice and Rights for individuals (Notice and Rights for individuals to the public).	Mandatory	COMPLETED
1.1.4 Your business processes.	Mandatory	COMPLETED

Sector baseline standard

High quality data source

DHSC assurance

Threat horizon scanning

Raising maturity
(achievable at a stretch)



DSP Toolkit for 22- 23



Transition to 22-23 Toolkit

**22-23 Standard
agreed and
available at:**

[https://www.dsptoolkit.nhs.uk/
News/22-23-DSP-Toolkit-
evidence-items](https://www.dsptoolkit.nhs.uk/News/22-23-DSP-Toolkit-evidence-items)

**Audit and Big
Picture guides
available now with
pdfs 😊**

**Deadline is
30th June
2023**

**Baseline 28th
February
2023 ICBs**

**Assertions
and
checkboxes
are unticked**

**Responses
from 22-23
transferred
where
evidence
item
unchanged**

**Evidence
item
numbers
have been
Reordered
and gaps
removed**

**Additional
Evidence
items for
ICBs**

22-23 DSP Toolkit – Key Changes

Incorporate IG Simplification

NHS E Privacy Team advice on removing duplication, aligning with updated guidance

ICB/ALB move to Category 1

Additional requirements for ICBs

Feedback Review

DSPT evidence items reviewed and updated based on feedback, support calls and comments from stakeholders. Evidence items reviewed

Tooltips expanded

More detail drawn from Audit guides

Audit requirements

Assertions to be Audited are: 1.3, 2.1, 3.4, 4.1, 4.2, 4.5, 5.1, 6.3, 7.2, 7.3, 8.3, 9.3 and 10.1

Consent requirement made mandatory

NHS E Privacy Team advice on removing duplication, aligning with updated guidance

Technical requirements strengthened

Specific Improvements to requirements on Medical Devices, ATP, vulnerabilities, unsupported systems, Early Warning Service and network documentation

Training

Change coming from since 1st July to the last 12 months.

**Where has the
wording been
tweaked (watch out
for date changes)**



3.2.1 Training requirement amendment coming...

<p>At least 95% of all staff, have completed their annual Data Security Awareness Training since 1st July 2022.</p>	<p>Please provide your highest percentage figure for the period 1st July 2022 - 30th June 2023 in the space below with an explanation of how you have calculated the figure.</p> <p>This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system. If using local training it must cover the areas included in https://portal.e-lfh.org.uk/Component/Details/544182</p> <p>All staff, which includes new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual Data Security Awareness Training (including passing a mandatory test).</p>
---	---

To

<p>At least 95% of all staff, have completed their annual Data Security Awareness Training in the last twelve months.</p>	<p>Please provide your percentage figure for the last twelve months prior to the date of publication, in the space below with an explanation of how you have calculated the figure.</p> <p>This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system. If using local training it must cover the areas included in https://portal.e-lfh.org.uk/Component/Details/544182</p> <p>All staff, which includes new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual Data Security Awareness Training (including passing a mandatory test).</p>
---	---



Examples of last twelve months before publication

Publication Date = 30.06.2023

Training included is:

01.07.2022 – 30.06.23

Publication date = 01.06.2023

Training included is:

02.06.2022 – 01.06.2023

Publication date = 01.04.2023

Training included is:

02.04.2022 – 01.04.2023

Publication date = 01.10.2022

Training included is:

02.10.2021 – 01.10.2022

Example Answer for 3.2.1 Training based on 1st June 2023 publication date

96.1% of staff have completed Data Security Awareness training in the last twelve months.

This was calculated as below:

Number of staff (including locums, temporary, students and staff contracted to work in the organisation) in the organisation = 10,000.

Number of staff completing data security awareness training since 2nd June 2022 = 9,610

Broken down into:

Number of staff completing national Data Security Awareness training = 8,140

Number of staff completing face to face IG session with test = 1,500

Number of staff completing data security awareness training with other organisations since 2nd June 2022 = 21

Number of staff figure is taken from email exchange with HR/Payroll team from 20/08/2021 which is available in the 22-23 DSPT Evidence – 3.2.1 Folder on SharePoint.

Number of staff completing face to face IG session with test, is taken from the registers of the session which are available in the 22-23 DSPT Evidence – 3.2.1 Folder on SharePoint.

Number of staff completing data security awareness training with other organisations since 2nd June 2022 is taken from the certificates/emails of the session which are available in the 21-22 DSPT Evidence – 3.2.1 Folder on SharePoint.



Integrated Care Boards



Completing the DSP Toolkit as an ICB

The ICB will be responsible for submitting a Data Security and Protection Toolkit (DSPT) for 22-23.

ICB Toolkit empty to begin with

ICBs are required to complete a DSP Toolkit Audit and complete a baseline

Scope of ICB Toolkit is the legal entity of the Integrated Care board not the patch.

Understood some might have zero Connected Medical Devices in your asset register but it is the checking that counts

ICBs and ODS Codes Watch out for this

ICBs have Q codes make sure you are completing the correct DSP Toolkit

If in doubt contact the Exeter helpdesk

CCGs not required to complete a DSPT

You may still access to old CCG DSPT don't just carry on with it 😊

Places are not required to complete a separate DSP Toolkit watch out for ODS Code changes in Old CCGs

Further reading at:

<https://digital.nhs.uk/services/organisation-data-service/upcoming-code-changes>

Responses



It is expected that some ICB responses may be made up of a CCG level responses so you can start work now.



For example you may in place ROPAs at a CCG level now and pull them together in a summary paper to an ICB group once established.



The key is to ensure there is a plan to harmonise the work towards an integrated ICB response.

To meet the DSP Toolkit in an ICB

1.1.2 Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Step 1 – Complete the Reviews

- Acceptable to have different information Asset registers and data flows systems across 'old' CCGs.
- Must follow the relevant guidance for data flows be undertaken since 01 July 2022

Step 2 – Documentation

- Acceptable for different format of reports to be produced following reviews
- Can be completed in pre-ICB format

Step 3 – ICB Reporting

Acceptable to have a summary report of all reviews presented to the ICB SIRO and the accountable group

ICB SIRO approve overall ICB registers and data flows.

ICB Queries - Connected Medical Devices

The ICB have any Connected Medical Devices how do we respond?

Explain the process you have been through to confirm you do not have any connected medical devices.

This could be by reviewing information asset registers confirmation for IT Suppliers etc.,

ICB Queries - Data Quality

What sort of DQ Board should the ICB set up?

It should cover the data you process and be proportionate.

The meeting's terms of reference are set by the organisation but you should document your decision

ICB Queries – Assurance statement from IT Suppliers

Can we use Assurance Statements from IT Suppliers as evidence for the DSP Toolkit now we are ICBs rather than CCGs?

Yes you can if it is appropriate.
For example; on whether software is being updated and patches are being applied.
No change from CCG publications

Help and Support



Resources to help

Monthly Webinars for Cat 1 organisations <https://www.dsptoolkit.nhs.uk/News/webinars>

helpdesk exeter.helpdesk@nhs.net.

Audit Guides

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

Useful as set out the requirement in a ISO 27001 style with

Security and Protection (DSP) Toolkit Strengthening Assurance Framework 2020- 298 / 637

Standard 5: Assertion 1

Mandatory

Process reviews are held at least once per year where data security is put at risk and following data security incidents.

Category	1	2	3	4
Control Objective	The organisation identifies the root cause of data security and protection incidents, in order to design and implement mitigating controls to either prevent similar incidents from occurring in the future or to be in a position to better manage them if they do occur.			
Approach	1. Review the organisation's data security and protection incident management procedure. Confirm that it includes a mechanism for identifying the root cause of an incident as part of the lessons learned exercise. 2. Select a sample of data security and protection incidents and confirm that the root cause of the incident has been identified. Review the nature of each of the sampled incidents and confirm that the root cause appears to be appropriate, and has associated mitigating actions assigned with ownership and implementation dates. 3. For the incidents sampled, confirm that controls have been implemented/enhanced, or other steps have been taken, to prevent similar incidents from occurring in the future.			
Assessment Documentation	1. Data security and protection incident management procedure. 2. Documentation associated with a sample of incidents with details on the root cause of the incident. 3. Evidence associated with action being taken to prevent similar incidents from occurring in the future.			

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



Remote Access Authentication

As remote access opens your resources (corporate networks and web applications) potentially to the entire internet it is important that all remote access has strong authentication.

Ideally this should be multifactor (normally 2 form) which normally takes the form of username / password and a hardware or soft token.

<https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>

All remote access is authenticated.

Data Security Standard 9.9

Protecting networked non internet devices

These are devices that are connected to your network (but not the internet) either because they are legacy systems, medical devices or untrusted systems that cannot be patched.

It is important you protect these systems and your wider network from each other. This can be accomplished through such techniques as:

- Network separation (such as VLAN's).
- Blacklisting.
- Virtualisation.
- Sandboxing.
- Separate firewall.
- Non-routable subnets.

Any questions?





NHS
Digital

Thank You



@nhsdigital



company/nhs-digital



digital.nhs.uk