

Data Security Protection Toolkit – Top Tips?



Information and technology
for better health and care

Presented by: John Hodson
NHS Digital

Data Security and Protection Toolkit in numbers

33 development sprints completed



9,000+

Registered organisations



11,600

Active Users



Integrated GDPR + NIS
Incident notification
for streamlined
automated reporting

Care
Homes

Uptake so far*

300+%



Feedback
items



Takes in account
other recognised
Certifications
and systems

380

GDPR Incidents
Reported to ICO



8

Bugs

Reported and fixed₂



What is coming Functionality

- Accessibility and User Interface Improvements
- Provide evidence for multiple organisations but not submitting (any volunteers to test?)
- Public View
- Enhanced reporting
- Generate an action plan

* Not exhaustive

Data Security and Protection Toolkit
Digital 2025 This is a new service - your feedback will help us to improve it.

Assessment - Trumpton Care NHS Foundation Trust

Progress

- 1 of 2 assessment criteria completed
- 2 of 128 remaining evidence items completed
- 8 of 44 questions completed

Your assessment status
If you want to submit your assessment

Go to your assessment results

You have until October 31st 2024 to complete this assessment.

1 Personal confidential data

2 Staff responsibilities

3 Policies

4 Alternative data sources

5 Finance systems

6 Planning to extend

7 Contracts

8 Connected systems

9 IT governance

10 Accessible systems

1. Personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely whether in electronic or paper form.
See the guidance on the Data Security and Protection Toolkit website.

Guidance Item 1.1.1

There is a data security and protection policy or policies that follow relevant guidance.

Confirm that you have policies in place that explain the organisation's plan or principles for data protection, data quality, records management, data security, retention activities and network security and refer to the organisation's procedures for implementing the policies.

Comments (optional)

The evidence will be applied to the following organisations

- TT000 - Trumpton Care NHS Foundation Trust
- TT001 - High Health Centre (Trumpton Care NHS Foundation Trust)
- TT002 - Challenge Practice (Trumpton Care NHS Foundation Trust)

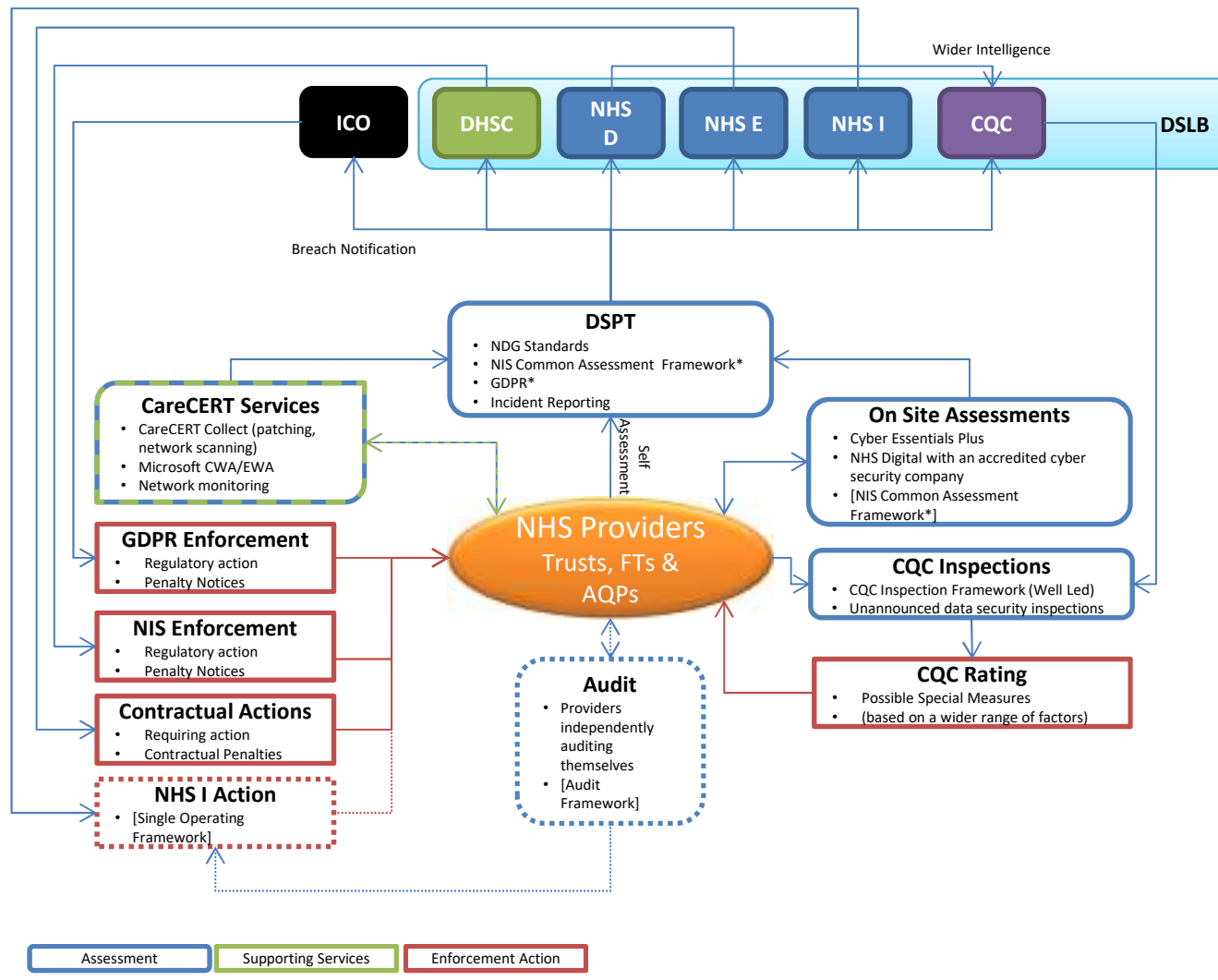
Search other organisations

Save and back to assessment Save and go to next evidence item

Overview of levels in the DSP Toolkit



Name	Description
Entry Level	Time-limited level (subject to review) for smaller organisations. Evidence items for critical legal requirements are being met; but some expected mandatory requirements have <u>not</u> been met. (https://www.dsptoolkit.nhs.uk/Help/32) Allows access to NHSmail.
Standards Met	Evidence items for all mandatory expected requirements have been met. Access to NHSmail, other secure national digital solutions, e.g. Summary Care Records, and potentially local digital information sharing solutions.
Standards Exceeded	Evidence items for all mandatory expected requirements have been met. The organisation has external cyber security accreditation. Evidence of best practice.
Critical Standards <u>Not</u> Met	Evidence items for critical legal requirements have <u>not</u> been met by the organisation. No access to information sharing tools e.g. NHSmail.





What is coming....continued

- October deadline for trust(s) to publish baseline
- Develop CQC Inspections and Audit
- Webinars <https://www.dsptoolkit.nhs.uk/News/10>
- Drive on take up especially in social care
- Prepare for next year



Iterative development

NHS Digital CareCERT Assurance Portal

Home | Progress Review | Data Security | Information Security | Information Governance | Data Protection | Data Security and Protection

Your Progress Review for 2017

Information Security | Data Security | Information Governance | Data Protection | Data Security and Protection

There is senior ownership of data security and protection within the organisation

1.1 There is senior ownership of data security and protection within the organisation

1.1.1 There is senior ownership of data security and protection within the organisation

1.1.2 There is senior ownership of data security and protection within the organisation

1.1.3 There is senior ownership of data security and protection within the organisation

1.1.4 There is senior ownership of data security and protection within the organisation

1.1.5 There is senior ownership of data security and protection within the organisation

NHS Digital Data Security and Protection Toolkit

Home | Assessment | Status | Report an Incident | Help | Contact Us

View: Health org 1 | Groups | Assessment | Incidents | Organisation Admin | News | Help

Assessment - Assertions

1.1 There is senior ownership of data security and protection within the organisation

1.1.1 There is senior ownership of data security and protection within the organisation

1.1.2 There is senior ownership of data security and protection within the organisation

1.1.3 There is senior ownership of data security and protection within the organisation

1.1.4 There is senior ownership of data security and protection within the organisation

1.1.5 There is senior ownership of data security and protection within the organisation

NHS Digital Data Security and Protection Toolkit

Home | Assessment | Incidents | Organisation Admin | News | Help

Viewing: Health org 1 | Groups | Assessment | Incidents | Organisation Admin | News | Help

2018 / 19 Assessment

The 2017/18 Data Security and Protection Requirements (opens in a new tab) define 10 Standards of data protection. Use this form to assess that your organisation adheres to them by providing evidence.

Progress

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

You have until April 5th 2019 to complete your assessment. [Read more about standard status.](#)

There are 172 remaining evidence items that are required to complete assertions. Once you have provided all the evidence for an assertion you must confirm that the provided information is correct. There are 32 assertions that need to be confirmed.

[Publish assessment as it is now](#)
[View a dashboard of your progress](#)

Filters

Mandatory

Mandatory (172)

Optional (00)

Status

Complete (7)

1. Personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.

[More about the personal confidential data standard \(opens in a new tab\)](#)

1.1 There is senior ownership of data security and protection within the organisation.

Owner: You, change

1.1.1 Name of senior information Risk Owner	Required
1.1.2 SIRM Responsibility for data security has been assigned.	Required
1.1.3 Name of Caldicott Guardian.	Required
1.1.4 Who are your staff with responsibility for data protection and/or security?	Required
1.1.5 Staff awareness - Leadership (C1) feel data security and protection are important for my organisation.	

Baseline

- Large NHS organisations (Acute, Ambulance Trust, Mental Health Trust, Community Trust) must publish a baseline by the end of October <https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0086-data-security-and-protection-toolkit-version-1-0>
- You won't be able to publish a baseline if:
 - You are not one of the above organisation types
 - You have not completed your profile
 - You have already published a full (standards met) assessment
- You can publish more than one baseline (but you don't have to)*
- Deadline 31st October midnight

Top Tips /1

- You can go back in and change any of the Org Profile Questions right up to publication.
- PSN and Cyber Essentials Certificate dates may need to be updated before publication
- Need to accept and submit any changes
- Work on Mandatory First
- Survey Questions are not Mandatory

Accept and Submit		
Sector Information		
Primary Sector	Domiciliary Care Organisation	Change
Key Role: Caldicott Guardian		
	Not Provided	Change
Key Role: SIRO		
	Not Provided	Change
Key Role: IG Lead		
	Not Provided	Change
Key Role: Data Protection Officer		
	Not Provided	Change
Mail System		
Is NHS Mail the only email system used by your organisation?	Yes	Change
Cyber Essentials PLUS		
Does your organisation have Cyber Essentials PLUS Certification with a scope covering all health and care data processing awarded during the last 12 months?	Yes	Change
Cyber Essentials PLUS award date	12/09/2017	
Cyber Essentials PLUS Certificate	Not provided	



Top Tips /2

- Administrators can create new users and set permissions
- Only Administrators can publish an assessment (or report incidents)
- Member users can add evidence (and confirm assertions where an administrator has made them an owner)
- Audit users are read only
- You can set up external users here
- If you manage more than one org you must select it to set up users.

Add user

Enter the email of the user you wish to add and the type of access (role) they require.

Email

Role

Administrator
For the people who need full access.

Member
Can edit evidence items but can not create new users, publish assessments or view/report incidents.

Auditor
Read only access to assessment.

[Add User](#)



Top Tips /3

- You can add links to evidence rather than upload it
- For LAs the scope is Adult Social Services and Public Health
- CQC Inspections so far have focussed on governance of information risk
- To meet the standard you must confirm all the mandatory assertions before you publish

1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.			
Owner: rux (Change)			
1.2.1	There is a data security and protection policy or policies that follow relevant guidance.	Mandatory	COMPLETED
1.2.2	When were the data security and protection policy or policies last updated?	Mandatory	COMPLETED
1.2.3	Policy has been approved by the person with overall responsibility for data security.	Mandatory	COMPLETED
1.2.4	Data Security and Protection Policies available to the public.		
1.2.5	Staff awareness – Policies (22): I know the facts about who I share data with and how.		COMPLETED
1.2.6	Staff awareness – Policies (22): I know who to ask questions about data security in my organisation.		COMPLETED
<input type="checkbox"/> I confirm that the evidence entered for this assertion is correct.			

Top Tips /4

- If inviting sites onto the DSPT send them
- <https://www.dsptoolkit.nhs.uk/Account/Register>
- Guidance for Coding, Service User Data, Smartcards
- Sites which have registered and/or published are available
<https://www.dsptoolkit.nhs.uk/News/34>)
- Document explaining DSPT levels
<https://www.dsptoolkit.nhs.uk/News/33>
-

E-Learning Top tips

- **Self-registration on e-learning for healthcare (e-LfH)** <https://nhsdigital.e-lfh.org.uk/>
- **Organisation registration**
<https://healtheducationyh.onlinesurveys.ac.uk/nhs-digital-data-security-awareness>
- **Access through Athens** (<http://portal.e-lfh.org.uk>)
- **More details** (<https://www.dsptoolkit.nhs.uk/Help/30>)

Help and Support

- Register
- <https://www.dsptoolkit.nhs.uk/Account/Register>
- Presentation developed to be used by IG Leads.
- <https://www.dsptoolkit.nhs.uk/News/25>
- FAQs including Training Tool.
- <https://www.dsptoolkit.nhs.uk/News/9>
- DSP Toolkit Support available through.
- Exeter.helpdesk@nhs.net
- Toolkit training and update events including presentations
- <https://www.dsptoolkit.nhs.uk/News/10>

Incident Reporting

- Tool Launched
- <https://www.dsptoolkit.nhs.uk/Incidents>
- Guidance Published
<https://www.dsptoolkit.nhs.uk/Help/29>
- Worked with ICO DHSC, NHS England and NHS
- Guidance updated including guidance on Annual reports.
- May need to update local policy to reflect changes

What is Changing

- The scoring system of SIRI has been changed
- Level 2 is no longer the trigger for reporting
- Number of people effected not a Sensitivity factors anymore
- Trigger for reporting is harm and impact
- Notification System not an Incident Management System

What is reportable ?

- ICO -The incident is assessed that it is (at least) likely that there is a risk to individual rights and freedoms (harm) and that the impact is (at least) minor
- DHSC - -The incident is assessed that it is (at least) likely that there is a risk to individual rights and freedoms (harm) and that the impact is (at least) serious.
- Where the 72 hours (real hours) deadline is not met an organisation must provide an explanation

Severity (Impact)	Catastrophic	5	5	10	15 20 25 DHSC & ICO		
	Serious	4	4	8	12 16 20		
	Adverse	3	3	6	9 12 15 ICO		
	Minor	2	2	4	6 8 10		
	No adverse effect	1	1	2	3	4	5
		1	2	3	4	5	
		Not Occurred	Not Likely	Likely	Highly Likely	Occurred	
		Likelihood that citizens' rights have been affected (harm)					

Factors to consider

- Type of breach
 - Nature, sensitivity and volume of personal data
 - How easy it would be identify the individuals
 - Potential consequences
-
- Look at the examples at the back of the guidance

What to report - Not ideal

- A patient letter was sent to the wrong address.

What to report - A bit better

- A letter was sent to a single patient of the physiotherapy service on 10th August. It has come to light that this was sent to the wrong address. The letter was opened, and all of the information included in the letter was read by another person who had no reason to view this data.
- The letter has been sent back to the Trust and returned to the department.

What to report - A bit better

- A physiotherapy appointment letter was sent from the Hospital dated 10th of August. This letter contained demographic details of the patient, a summary of the medical condition of the patient, a brief patient history and a list of other appointment's that the patient has in the next few months as a reminder. This will contain sensitive personal information.
- The person who opened the letter has the same surname as the patient and may be a family member.
- An initial investigation has identified that this was an individually typed letter so the issue is unlikely to be replicated widely across the service. It was individual letter as the appointment was being rearranged. As the patient didn't receive information about the appointment they missed their appointment, so it will have to be rearranged delaying the start of their treatment.
- The DPO , Caldicott Guardian have been informed and the incident has been recorded on the internal incident reporting system.
- We are speaking to the Physio service manager and the patient to provide the earliest possible appointment to minimise the impact.
- We have spoken to the patient to explain what has happened and apologies. A written apology is also being drafted to be signed by the Head of Service.
- Key Contacts for the incident is john.smaith@nhs.com 01111 111111.



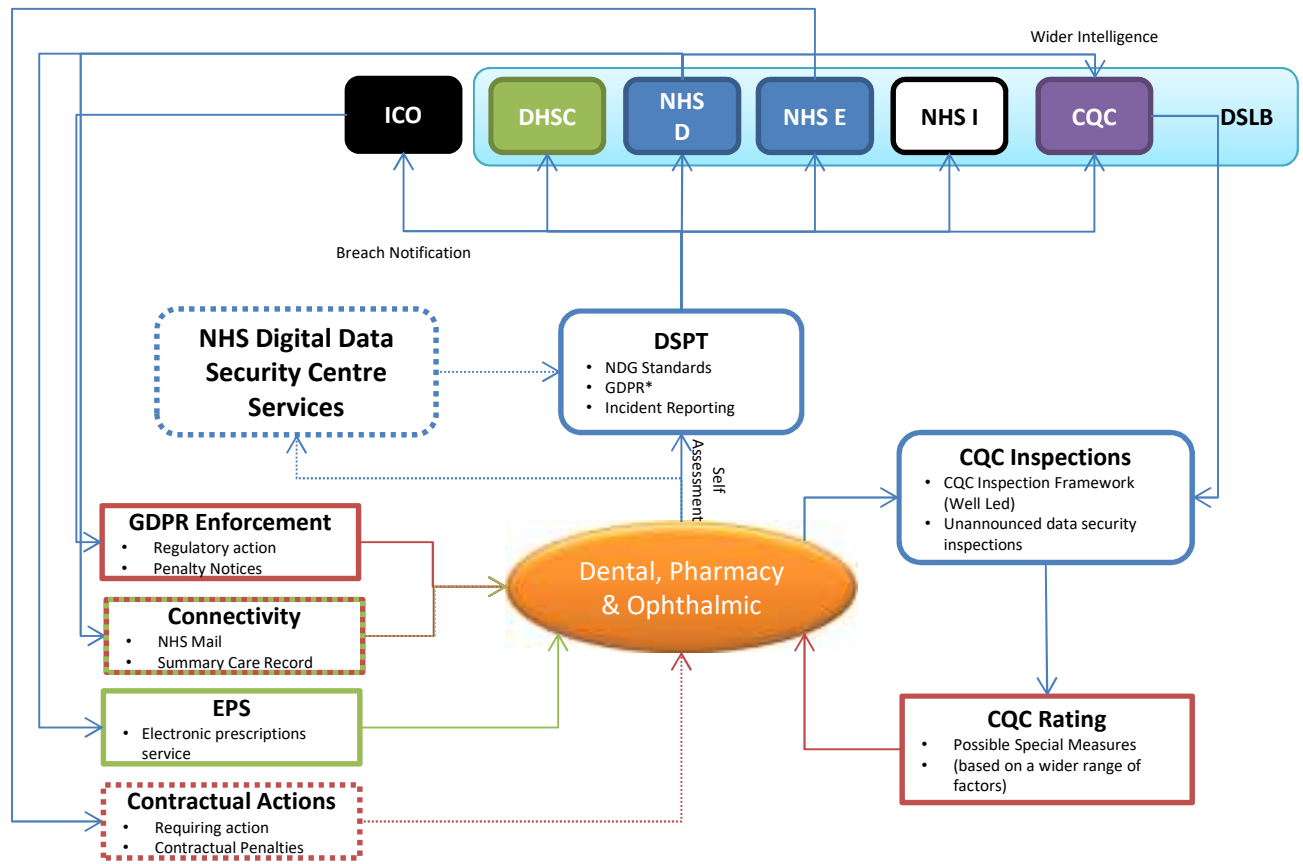
www.digital.nhs.uk

 [@nhsdigital](https://twitter.com/nhsdigital)

enquiries@nhsdigital.nhs.uk

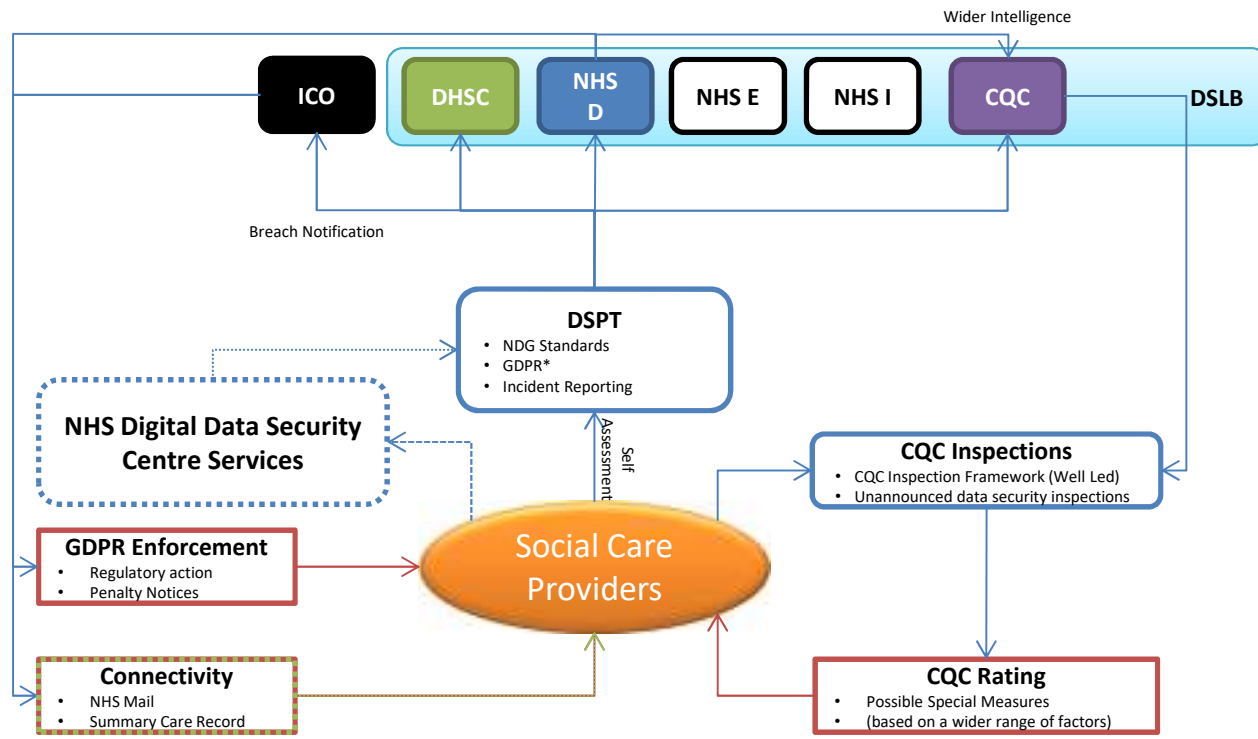
0300 303 5678

Information and technology
for better health and care



K
e
v





K
e
v

