

Data Security Protection Toolkit – Overview?

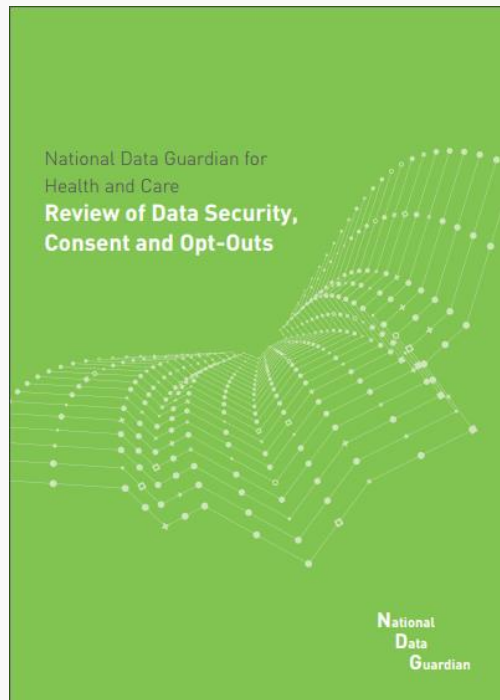


Information and technology
for better health and care

Presented by: David Ingham
& John Hodson
NHS Digital

Why data security is important

- It's about Trust!
- “Trust cannot be ensured without secure systems...”
- People trust the health and care system to protect information.
- Data Security must support digital transformation otherwise the risk of breaches increase and trust will be lost.



Data Security & Protection Toolkit in numbers

28 development
sprints completed



6,800+
active user organisations



Active
Users



Integrated GDPR + NIS
Incident notification
for streamlined
automated reporting

**44 Higher
education
registrations**



Feedback
items



Takes in account
other recognised
Certifications
and systems

446 GDPR
Incidents
Recorded



3 Bugs

Reported and fixed₃

Iterative Development

NHS Digital CareCERT Assurance Portal

Home Progress Review CareCERT Incident Reporting Knowledge Share Training News & Resources Help Admin

Admin User 2 - Demo Organisation 2 [Skip Out](#)

Your Progress Review for 2017

View Organisation Profile Last saved by Admin User 2 on 18/04/2017 14:05

Summary Assertions Evidence Actions Reporting

NDG 1 - People National Data Guardian 1 - People: Responsibility and accountability for data security
There is senior ownership of data security and protection within the organisation

Assign Owner Standards [Go](#) Themes [Go](#)

Evidence

This is a list of evidence necessary to meet this requirement

Description	Type	Evidence Provided	Comments
✓ Caldicott Guardian is appointed	Text	appointment letter	appointment letter Edit Close
Date each risk was last reviewed by the board	Date		Edit Close
Dates of board discussions of the data security risk	Date		Edit Close
SIRO is a member of the board	List		Edit Close
SIRO Name	Text		Edit Close
Staff survey - Leadership (Q1)	Text		Edit Close
Staff with responsibility for data protection and/or security are identified	Attachment		Edit Close
Top three data security risks	Text		Edit Close

NDG 2 - People
NDG 3 - People
NDG 4 - Process

NHS Digital Data Security and Protection Toolkit

This is a new service - your feedback will help us to improve it.

Assessment News Report an Incident Help Admin

John Hodson - Small Org Test [Change Organisation](#) [Log Out](#)

Assessment - Assertions (38)

Filter By [Reset](#)

NDG Standard

- ☐ Personal Confidential Data (1)
- ☐ Staff Responsibilities (1)
- ☐ Training (1)
- ☐ Managing Data Access (1)
- ☐ Process Reviews (1)
- ☐ Responding to Incidents (1)
- ☐ Continuity Planning (1)
- ☐ Unsupported Systems (1)
- ☐ IT Protection (1)
- ☐ Accountable Suppliers (1)

Mandatory

- ☐ Mandatory (1)
- ☐ Not Mandatory (1)

Status

- ☐ Met (1)
- ☐ Not Met (1)
- ☐ Other (1)

Confirmed

- ☐ Not Confirmed (1)

Owner

- ☐ No Owner (1)
- ☐ John Hodson (1)

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

Owner:

Name of Senior Information Risk Owner: [Mandatory](#) [Completed](#)

SIRO Responsibility for data security has been assigned: [Mandatory](#)

Name of Caldicott Guardian: [Mandatory](#) [Completed](#)

Who are your staff with responsibility for data protection and/or security? [Mandatory](#)

Staff awareness - Leadership (Q1) I feel data security and protection are important for my organisation. [Mandatory](#) [Completed](#)

Name of Appointed Data Protection Officer: [Mandatory](#) [Completed](#)

Confirmed: No

Mandatory evidence must be completed before confirmation.

Assertion:
There are clear data security and protection policies in place and these are understood by staff and available to the public.

Owner:

NHS Digital Data Security and Protection Toolkit

This is a new service - your feedback will help us to improve it.

Account Logout

Viewing: Health org 1 [Change](#) [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 assert that your organisation adheres to them by providing evidence.

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 protections
10. Accountable suppliers

Progress

☐ ☐ ☐ ☐ ☐

If you were to publish now your status would be:

[Not submitted](#)

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](#)

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 SIRO 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 (Q1) I feel data security and protection are important for my organisation.	

Filters

Mandatory

☐ Mandatory (172)

☐ Optional (80)

Status

☐ Complete (0)



What is coming

- New functionality in development*
 - Amendment to Org Profile (Department)
 - Accessibility and User Interface Improvements
 - Provide evidence for multiple organisations but not submitting
 - Public View
 - Peer benchmarking & enhanced reporting
 - Generate an action plan

* Not exhaustive

Levels

Name	Description
★ Standards Exceeded	<ul style="list-style-type: none">• Evidence Items for all mandatory expected requirements have been met.• The organisation has external cyber security accreditation.• Evidence of best practice.
✓ Standards Met	<ul style="list-style-type: none">• Evidence items for all mandatory expected requirements have been met.• Required for access to NHS Digital Data• Equivalent to Satisfactory.
✗ Critical Standards Not Met	<ul style="list-style-type: none">• Evidence items for critical legal requirements have <u>not</u> been met by the organisation.• No access to information sharing tools e.g. NHS Digital Data.

Incident Reporting

- Tool Launched
- <https://www.dsptoolkit.nhs.uk/Incidents>
- Guidance Published and updated
<https://www.dsptoolkit.nhs.uk/Help/29>
- Worked with ICO DHSC, NHS England and NHS
- Any comments or suggestions about the guidance email us on cybersecurity@nhs.net

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 some harm has occurred and that the impact is (at least) minor,
- DHSC - The incident is (at least) likely that harm has occurred and the impact is at least serious.
- Where the 72 hours (real hours) deadline is not met an organisation must provide an explanation
- Look at the examples at the back of the guidance

Impact	Catastrophic	5	5	10	15 20 25 Reportable to the ICO DHSC Notified		
	Serious	4	4 No Impact has occurred	8 An impact is unlikely	12 16 20		
	Adverse	3	3	6	9 12 15 Reportable to the ICO		
	Minor	2	2	4	6 8 10		
	No Impact	1	1 2 No Impact has occurred 3 4 5				
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				

E-Learning

- **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

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
- <https://www.dsptoolkit.nhs.uk/News/10>

The background of the slide is an abstract composition of light. It features a dense field of out-of-focus circular bokeh in shades of blue and purple. Overlaid on this are numerous bright, elongated streaks of light, primarily in magenta and pink, that appear to be moving or falling from the top right towards the bottom left. The overall effect is dynamic and futuristic.

Demonstration



Questions?

cybersecurity@nhs.net

www.digital.nhs.uk

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

enquiries@nhsdigital.nhs.uk

0300 303 5678

Information and technology
for better health and care