NHS Digital

DSP Toolkit

Update for NHS Trusts, CCGs and CSUs

Webinar begins at 12.30.
Please mute your microphones.

June 2021
John Hodson

Information and technology
for better health and care

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

Key Messages

- Deadline 30th June 2021
- Improvement plan guidance launched
- CE+ Onsite Assessment not a mandatory requirement.
- National Data Opt out date has been extended to September for 1.4.4 is being made non-mandatory
- Spot checks (1.5.2) are not required to be physical can be digital or remote.
- Training requirement 3.2.1check the tooltip

20-21 DSP Toolkit

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

Cyber Essentials + and DSP Toolkit

- The requirement to have an On-site assessment by 30 June 2021 is no longer mandatory.
- The questions of Cyber Essentials have been incorporated into the Toolkit for NHS Trusts Standards met it is the ‘+’ element which relates to the On-site assessment.
- Updated comms on news page https://www.dsptoolkit.nhs.uk/News/91

DSP Toolkit 20-21 NHS Trusts, Newly Mandatory

1.7.3	A data quality forum monitors the effectiveness of data quality assurance processes.	8.3.4	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.
4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	9.1.2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.
4.2.5	Are unnecessary user accounts removed or disabled?	9.3.2	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.
4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	9.6.5	End user devices are built from a consistent and approved base image.
4.5.3	Multifactor authentication is used [wherever technically feasible].	9.6.6	End user device security settings are managed and deployed centrally.
6.2.5	Antivirus/anti-malware software scans files automatically upon access.	9.6.7	AutoRun is disabled.
6.2.6	Connections to malicious websites on the Internet are prevented.	9.6.10	You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted and signed off by the SIRO.
7.3.5	When did you last successfully restore from a backup?	9.7.2	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?
7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	9.7.5	Have firewall rules that are no longer required been removed or disabled?
8.1.3	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.	9.7.6	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

DSP Toolkit 20-21 CCG/CSU, Newly Mandatory

4.2.5	Are unnecessary user accounts removed or disabled?
6.2.3	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?
7.3.5	When did you last successfully restore from a backup?
7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose
8.3.4	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.
9.7.1	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

DSP Toolkit 20-21 (Small organisations)

- All mandatory evidence items updated
- Worked with IPC and organisations who haven't completed a toolkit before to improve wording, on screen guidance and links to support materials.
- Additional requirements on records, passwords and mobiles.
- Dedicated support for social care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/data-security-and-protection-toolkit/

Evidence item 3.2.1

- Have at least 95% of all staff, completed their annual Data Security Awareness Training?

- Please provide your highest percentage figure for the period 1st April 2020 - 30th June 2021 in the space below with an explanation of how you have calculated the figure.
- This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system.

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

Evidence item 3.2.1

- Include training undertaken between 1st April 2020 – 30th June 2021 not only since the Toolkit had been published. So If a member of staff completed training on 25th September 2020 and you included them in your figures for last year, you could include them in this year's figures as well as last years.

- It can be your ‘best’ score.

- You can use your own training package as long as it covers the same learning objectives, signed off by SIRO or CG and has a test which staff must pass.

- Learning objectives available https://portal.e-lfh.org.uk/Component/Details/544182

Top Tips

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

- Check your owners of each assertion are still correct
- Check your Organisation Profile before you publish as it will save stress on publication.
- National Data Opt out date has been extended to September for 1.4.4 is being made non-mandatory
- Spot checks (1.5.2) are not required to be physical can be digital or remote.

What is stopping you publishing?

- Not all Mandatory evidence items answered
  - Or only responded to in the comment box
- Assertions with mandatory evidence items not confirmed.
- No Administrator set up
- Owners set up but not around
- Change in Organisation profile not confirmed
- Forgotten password
- Branches not selected

DSP Toolkit Updates

Audit Guides

Key messages

Facts and Figures

DSP Toolkit 20-21

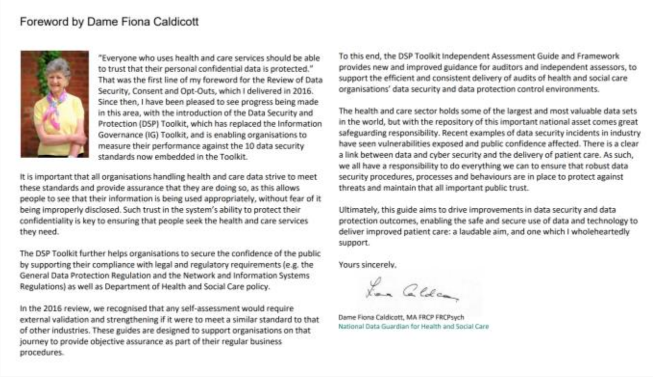
Updates

Support

ta Security and Protection (DSP) Toolkit Strengthening Assurance Framework 2020... 1 / 637
NHS
Digital

Strengthening Assurance

Data Security and Protection (DSP) Toolkit
Independent Assessment Framework



Foreword by Dame Fiona Caldicott

"Everyone who uses health and care services should be able to trust that their personal confidential data is protected." That was the first line of my foreword for the Review of Data Security, Consent and Opt-Outs, which I delivered in 2016. Since then, I have been pleased to see progress being made in this area, with the introduction of the Data Security and Protection (DSP) Toolkit, which has replaced the Information Governance (IG) Toolkit, and is enabling organisations to measure their performance against the 10 data security standards now embedded in the Toolkit.

It is important that all organisations handling health and care data strive to meet these standards and provide assurance that they are doing so, as this allows people to see that their information is being used appropriately, without fear of it being improperly disclosed. Such trust in the system's ability to protect their confidentiality is key to ensuring that people seek the health and care services they need.

The DSP Toolkit further helps organisations to secure the confidence of the public by supporting their compliance with legal and regulatory requirements (e.g. the General Data Protection Regulation and the Network and Information Systems Regulations) as well as Department of Health and Social Care policy.

In the 2016 review, we recognised that any self-assessment would require external validation and strengthening if it were to meet a similar standard to that of other industries. These guides are designed to support organisations on that journey to provide objective assurance as part of their regular business procedures.

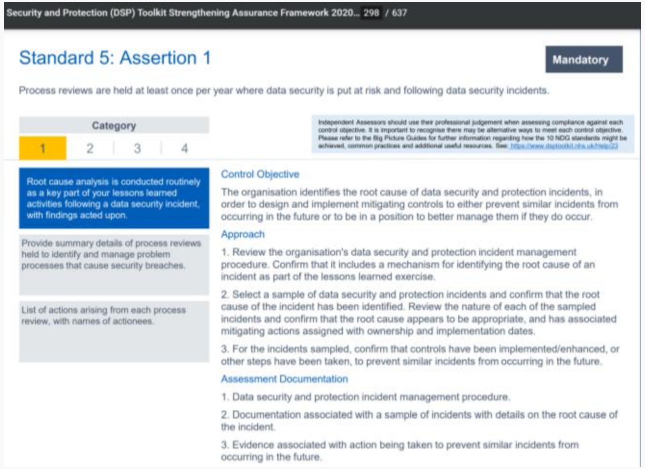
To this end, the DSP Toolkit Independent Assessment Guide and Framework provides new and improved guidance for auditors and independent assessors, to support the efficient and consistent delivery of audits of health and social care organisations' data security and data protection control environments.

The health and care sector holds some of the largest and most valuable data sets in the world, but with the repository of this important national asset comes great safeguarding responsibility. Recent examples of data security incidents in industry have seen vulnerabilities exposed and public confidence affected. There is a clear a link between data and cyber security and the delivery of patient care. As such, we all have a responsibility to do everything we can to ensure that robust data security procedures, processes and behaviours are in place to protect against threats and maintain that all important public trust.

Ultimately, this guide aims to drive improvements in data security and data protection outcomes, enabling the safe and secure use of data and technology to deliver improved patient care: a laudable aim, and one which I wholeheartedly support.

Yours sincerelv.

Dame Fiona Caldicott, MA FRCP FRCPsych
National Data Guardian for Health and Social Care


Security and Protection (DSP) Toolkit Strengthening Assurance Framework 2020... 298 / 637
Mandatory
Category
1
2
3
4

Standard 5: Assertion 1

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

Independent Assessors should use their professional judgement when assessing compliance against each control objective. It is important to recognise there may be alternative ways to meet each control objective. Please refer to the Big Picture Guides for further information regarding how the 10 NDG standards might be achieved, common practices and additional useful resources. See: https://www.dsptoolkit.nhs.uk/Help/23

Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon.

Provide summary details of process reviews held to identify and manage problem processes that cause security breaches.

List of actions arising from each process review, with names of actionees.

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.

Key messages

Facts and Figures

DSP Toolkit 20-21

Updates

Support

Support

Overview and user guide https://www.dsptoolkit.nhs.uk/Help/3

Helpdesk exeter.helpdesk@nhs.net https://www.dsptoolkit.nhs.uk/Home/Contact

Step by Step guide with Templates and examples
https://www.digitalsocialcare.co.uk/latest-guidance/completing-standards-met-on-the-data-security-and-protection-toolkit/

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

Big Picture guides
https://www.dsptoolkit.nhs.uk/Help/5

Audit guides https://www.dsptoolkit.nhs.uk/Help/64

Improvement Plans https://www.dsptoolkit.nhs.uk/News/improvement-plans

NHS
Digital

Connect with us

@nhsdigital

company/nhs-digital

www.digital.nhs.uk

Information and technology
for better health and care