Data Security and Protection Toolkit
Version 2
DCB0086 Requirements Specification

Published 29 May 2019

Information and technology
for better health and care

Amendment History:

Version	Date	Amendment History
0.1	27 February 2019	First draft
0.2	5 March 2019	Second draft – amended in response to feedback from Alan Morton and latest understanding of required CE PLUS position.
0.3	8 March 2019	Third draft – DHSC feedback incorporated
0.4	18 March 2019	Fourth draft – SME feedback incorporated
1.0	24 May 2019	Final version

Approvals:

This document must be approved by the following:

Name	Organisation	Title / Responsibility	Date	Version
Daniel Taylor	NHS Digital	Associate Director, Data Security Centre Senior Responsible Owner	07 March 2019	0.2
Katie Farrington	Department of Health and Social Care	Director of Technology, Digital and Data Sponsor	07 March 2019	0.2

Data Coordination Board

This information standard (DCB0086) has been approved for publication by the Department of Health and Social Care under section 250 of the Health and Social Care Act 2012.

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guide
- Change Specification.

An Information Standards Notice (DCB0086 Amd 9/2019) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 29 May 2019

Contents

1. Overview

This Requirements Specification is the formal definition of the Data Security and Protection (DSP) Toolkit Standard.

This document includes the scope of the standard, conformance requirements and timescales for data collection.

2. Glossary

Term	Acronym	Definition/ Link
Arm's Length Body	ALB	An organisation that delivers a public service, is not a ministerial government department, and which operates to a greater or lesser extent at a distance from Ministers e.g. executive agencies such as the Medicines and Healthcare Products Regulatory Agency; special health authorities such as the NHS Business Services Authority
Any Qualified Provider	AQP	AQP services include Musculo-skeletal services for back and neck pain; Adult hearing aid services in the community; Continence services (adults and children); Diagnostic tests closer to home such as some types of imaging, cardiac and respiratory investigations; Wheelchair services; Podiatry services; Venous leg ulcer and wound healing; Primary care psychological therapies (adults).
Care Quality Commission	CQC	See: http://www.cqc.org.uk/about-us Details of inspection regime, including Well-Led key lines of enquiry are available from: https://www.cqc.org.uk/guidance-providers/healthcare/key-lines-enquiry-healthcare-services
Data Access Request Service	DARS	See: https://digital.nhs.uk/services/data-access-request-service-dars

Data Protection Act 2018	DPA	See https://www.gov.uk/data-protection The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
The Department of Health and Social Care	DHSC	See https://www.gov.uk/government/organisations/department-of-health-and-social-care/about The Department of Health and Social Care (DHSC) supports Ministers in leading the nation's health and social care to help people live more independent, healthier lives for longer.
General Data Protection Regulation	GDPR	European Union Regulation see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
Confidentiality Advisory Group - Health Research Authority	HRA CAG	See: https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/
Information Governance Toolkit	IG Toolkit	Predecessor system to the Data Security and Protection Toolkit. See: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf
Data Security and Protection Toolkit	DSP Toolkit	Scope / Purpose as defined in this document
The Information Commissioner's Office	ICO	See https://ico.org.uk
Local Authorities	LA	A county, shire, district, borough or city council responsible for providing public services (including public health teams and adult social care delivery functions) within a defined geographical area.

National Data Guardian	NDG	The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly. https://www.gov.uk/government/organisations/national-data-guardian
NHS Business Partner	Not Applicable	An organisation that, whilst remaining independent, works closely with NHS organisations and shares common goals for providing high standards of healthcare directly to patients. The category includes some Independent Treatment Centres and DHSC Arm's Length Bodies
NHS Digital	NHS Digital	The national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care. The Health and Social Care Information Centre is a non-departmental body created by statute, also known as NHS Digital.
NHS England	NHSE	An executive non-departmental public body, sponsored by the Department of Health and Social care, See https://www.england.nhs.uk/about/
Sensitive Personal Data	N/A	Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation
Secondary Use Organisation	N/A	An organisation that processes patient information for secondary purposes.
Registration Information	N/A	Any information held by a registration official in the exercise of his or her registration functions – e.g. information held relating to births, adoptions, stillbirths, marriages, civil partnerships, gender and deaths.

3. Related/Supporting Information

The following documents, (available from the relevant links) provide a background to this standard, including the mandate for the DSP Toolkit and current policy:

- National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016
- Government Response "Your Data: Better Security, Better Choice, Better Care" July 2017
- Department of Health and Social Care "2017/18 Data security and protection requirements" October 2017
- Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR)

4. Definition

The Data Security and Protection (DSP) Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements set by the Department of Health and Social Care.

The DSP Toolkit has been developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017 (see section 3).

The DSP Toolkit is the successor framework to the IG Toolkit.

5. Background

The DSP Toolkit is a Department of Health and Social Care (DHSC) policy delivery vehicle that NHS Digital is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DHSC policy and presents them in a single standard as a set of requirements. Relevant organisations[1] are required to carry out self-assessments of their compliance against the assertions and evidence items contained within the DSP Toolkit.

5.1 Requirements

The DSP Toolkit provides a mechanism for organisations to assess themselves against the NDG 10 data security standards[2], through confirming assertions, and providing supporting evidence (details are provided at Appendix 1 - Assertions and evidence items).

Several assertion statements are identified, relevant to each of the 10 standards. Assertions are positive statements which organisations must review and (where appropriate) confirm.

[1] See section 7 (Scope)
[2] As defined in the National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

Each assertion is underpinned by one or more evidence items. These are pieces of information which (where appropriate) should be provided, to evidence assertions. These evidence items can be: a date, a document, yes/no confirmation, a number or text.

Some evidence items are considered a minimum expectation which an organisation must have in place. These are indicated as “mandatory” elements on the DSP Toolkit.

The use of “mandatory” functionality aims to ensure attention is focused on those highest priority elements of data security and information governance, whilst providing opportunity for organisations to evidence improvement over time against recommended elements. The recommended elements may become mandatory in future years to improve data security in organisations as data security maturity increases or threats change.

Requirements differ for different organisation types, to reflect data security risk, IT arrangements and digital maturity, see section 8.

Some relevant evidence items will not be required where an organisation uses NHSmail, or has in place an existing relevant standard (Cyber Essentials PLUS, ISO 27001, Public Service Network Information Assurance) where this standard is of an equivalent or higher level than the DSP Toolkit.

5.2 Purpose

The purpose of the assessment is to enable organisations to measure their compliance against the law (see 11.2) and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures to raise standards.

The aim is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of information. This in turn increases public confidence that the NHS and its partners can be trusted with their sensitive data.

For more information on the legal position / mandate, please see section 11.

5.3 Scope (overview)

DSP Toolkit assessments must be completed and published by organisations which:

- have access to NHS patients and/or to their information;
- provide support services directly to an NHS organisation; or
- have either direct or indirect access to national informatics services.

Further detail on who must complete a DSP Toolkit and its scope is provided in section 7.

5.4 Completing the DSP Toolkit in support of applications for section 251 approval and requests to the NHS Digital Data Access Request Service

All bodies (new and existing applicants) that are seeking access to NHS patient information via section 251 NHS Act 2006 applications to the approving body the Confidentiality Advisory

Group - Health Research Authority (HRA CAG) are required to provide IG assurances, part of which is submission of a DSP Toolkit assessment and to demonstrate a satisfactory level of compliance.

NHS Digital has taken similar measures in relation to requests for patient data for secondary uses (requests via the Data Access Request Service – DARS). Applicants must provide assurance that good Information Governance practices are being maintained by:

Providing assurance that your organisation meets the NHS Digital requirements and standards for specified controls (details of which must be provided to DARS directly).

And at least one of the following:

- Completing a DSP Toolkit assessment and meeting a satisfactory level of attainment; or
- Providing details of certification against the relevant international security standard (ISO); or
- Demonstrating that other assurances are in place (details of which must be provided to DARS directly).

Any dissemination of patient data for secondary use must also be approved through the DARS process and according to the policies and procedures set out through DARS and supported by Data Sharing Agreement (DSA) and Data Sharing Framework Contract.

NHS Digital will continue to provide assurances to DARS and HRA CAG.

6. Benefits

The DSP Toolkit provides a mechanism for organisations to demonstrate that they can be trusted to maintain the confidentiality and security of personal information. This in turn increases public confidence that ‘the NHS’ and its partners can be trusted with personal information. Organisations can publicise their DSP Toolkit assessment to demonstrate they are meeting the NDG Data Security Standards. It is hoped that increased personal confidence will minimise the number of individuals who 'opt out' of the sharing of their personal identifiable data.

The DSP Toolkit enables organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

By assessing themselves against the standard and implementing actions to address shortcomings identified though use of the DSP Toolkit, organisations should be able to reduce the risk of a data breach.

The General Data Protection Regulation allows the supervising authority (the Information Commissioner’s Office) to levy a maximum fine of €20,000,000 or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year whichever is greater.

7. Scope

Assessments must be completed and published by all bodies that process the personal confidential data of citizens which access health and adult social care services. These include, but are not limited to:

- NHS organisations (acute trusts, ambulance trusts, mental health trusts, clinical commissioning groups) including foundation trusts and NHS community health providers.
- NHS England.
- NHS Digital.
- Public Health England.
- Local Authority Adult Social Care.
- Local Authority Public Health.
- Primary Care providers (community pharmacies / dispensing appliance contractors, dental practices, eye care services, general practices).
- DHSC arm's length bodies that closely support care services (i.e. executive agencies such as the Medicines and Healthcare Products Regulatory Agency; special health authorities such as the NHS Business Services Authority).
- Bodies commissioned or otherwise contracted to provide services by any of the above.

In addition to the NHS mandate above, other organisations are required to provide Data Security and Protection assurances via the DSP Toolkit as part of business/service support processes or contractual terms. That is, for these organisations annual DSP Toolkit assessments are required for either or both of two purposes:

- To provide Data Security and Protection assurances to the Department of Health and Social Care or to NHS commissioners of services;
- To provide Data Security and Protection assurances to NHS Digital as part of the terms and conditions of using national systems and services including the e- Referral Service and NHSmail.

8. Requirements by User Group

The assertions which must be confirmed, and the evidence items which must be provided, vary by organisation type.

Each organisation type is automatically allocated a classification as follows:

Category 1: NHS trusts

Category 2: Arm's Length Bodies, CCGs and CSUs

Category 3: All other sectors (which do not fall under category 1, 2 or 4).

Category 4: GP Practice

The assertions which must be provided by each organisation classification are outlined in Appendix 1 - Assertions and evidence items.

9. Conformance

Relevant organisations[3] MUST publish their assessment via the DSP Toolkit annually by 31 March (full conformance date).

To publish an assessment via the DSP Toolkit:

a) Evidence MUST be provided against each mandatory evidence item (as defined in Appendix 1 - Assertions and evidence items).

b) Every assertion which includes one or more mandatory evidence item MUST be confirmed.

A published assessment meeting the above criteria constitutes a “Standards Met” assessment.

All organisations providing services under an NHS Standard Contract are required to undertake an audit on their DSP Toolkit submissions. Organisations registered with the CQC will have data security included in their Well-Led inspection with their DSP Toolkit considered as key evidence.

10. Timescales/Plan

10.1 First-time assessments

Organisations carrying out their first assessment should complete this in line with the contract of services they are party to, or as required by the tendering process they are involved in.

Where a first assessment is being carried out as part of an application for national systems and services, the organisation should complete this as soon as they are able as connection will not be granted until an assessment has been published and reviewed by NHS Digital.

Similarly, for Research Teams or National Registers required to complete a DSP Toolkit assessment in support of an application to access patient information held on national systems, held by NHS Digital or required for processing without consent (for both research and non-research purposes), the DSP Toolkit assessment should be completed within given timelines determined by the approval processes concerned (e.g. section 251 approvals by the Health Research Authority Confidentiality Advisory Group).

10.2 Additional assessments

A second or subsequent assessment can be started at any time but in all cases the final publication must be made online by 31 March each year.

Category 1 and 2 NHS organisations[4] are also required to complete an interim assessment during the year – the deadline for the interim submission will be 31 October each year. This

[3] See section 7 (Scope)
[4] See paragraph 8

will be publicised by writing to all the organisations covered by the scope of the interim assessments and by communication through the Strategic Information Governance Network, the network of IG leads in large health and care organisations.

The work necessary to make improvements or to maintain compliance should be an on-going process and not left till the year end.

Organisations registered with the CQC will have data security included in their Well-Led inspection with their DSP Toolkit considered as key evidence.

11. Legal Position / Mandate

11.1 Overview

It is Department of Health and Social Care policy that all organisations which have access to NHS patient information must provide assurances that they are practising good information governance and use the DSP Toolkit to evidence this by the publication of annual assessments.

It is also a contractual requirement in the NHS Standard contract[5] (general conditions section 21.2) that relevant providers[6] undertake DSP Toolkit assessments on an annual basis: "The Provider must complete and publish an annual information governance assessment and must demonstrate satisfactory compliance as defined in the Information Governance Toolkit (or any successor framework), as applicable to the Services and the Provider's organisation type."

It remains Department of Health and Social Care policy that all bodies that process NHS patient information for whatever purpose should provide assurance via the DSP Toolkit.

Use of the DSP Toolkit is also required as part of the DHSC publication: Data security and protection for health and care organisations October 2017.

NHS Digital has been directed to undertake this collection by the Department of Health and Social Care through a legal direction. Details are available from:

https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/data-security-and-protection-toolkit-data-collections-service

11.2 Related legislation, policy and good practice

In addition to the above, the standard (and associated guidance) draws together key rules and good practice about how information is handled pertaining to:

- The General Data Protection Regulation May 2018.
- The Data Protection Act 2018.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.

[5] https://www.england.nhs.uk/nhs-standard-contract/
[6] Those organisations which are subject to the terms of the NHS England standard contract

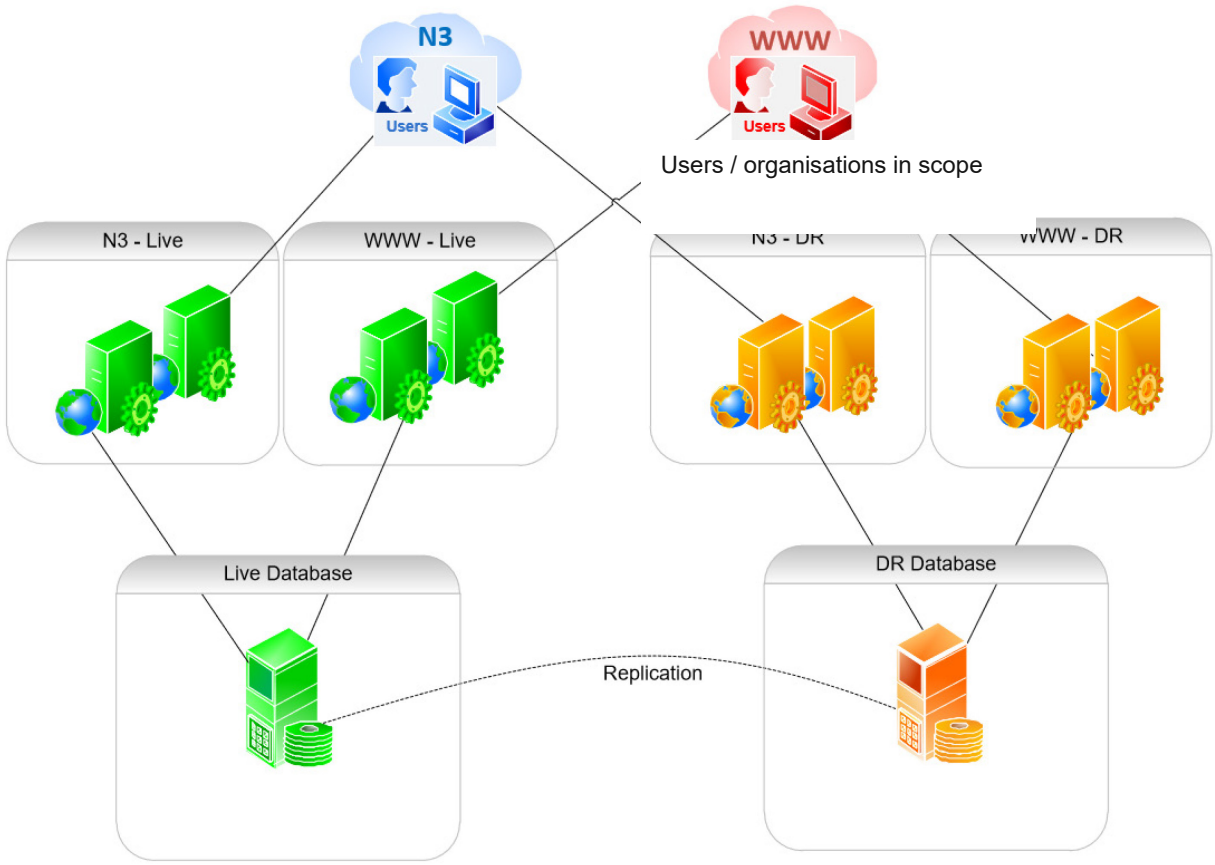
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review' (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2 Review
- Lessons learned review of the WannaCry Ransomware Cyber Attack (NHS England February 2018)

12. Data Flow

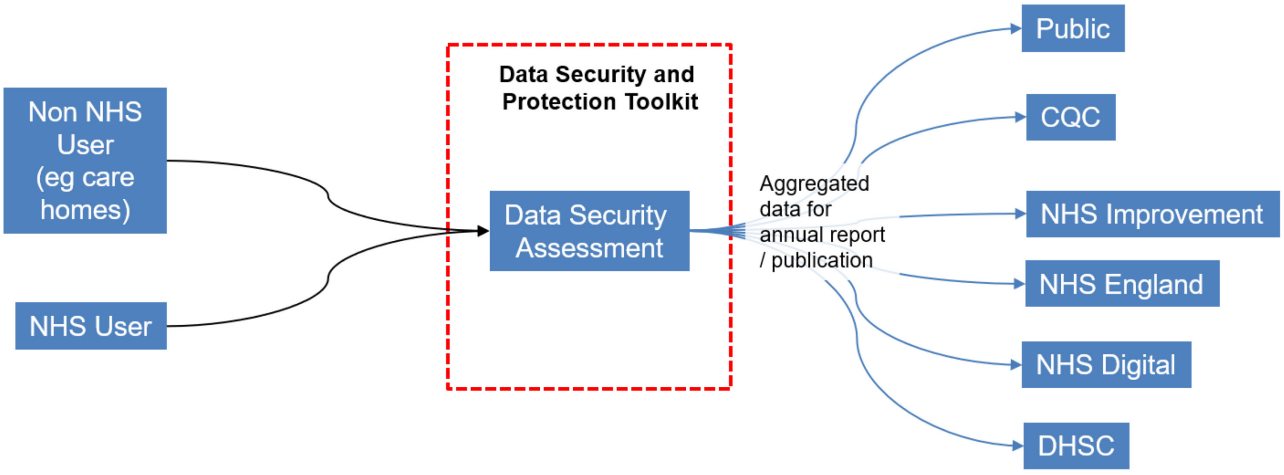
The DSP Toolkit is available to all users via a www domain: https://www.dsptoolkit.nhs.uk/ .

In accordance with the NHS Digital Infrastructure Platform Strategy it is intended that the solution is migrated to a cloud solution during 2019. This change will be communicated to users in advance of implementation.

The logical architecture is shown below.



Data flows are summarised as follows:



13. Data Set

The data captured by the system comprises:

- Dates
- Text (including contact details, narrative)
- Yes/No confirmations
- KPIs (e.g. values of fines, number of incidents, percentage of suppliers with relevant contract clauses)
- Documents (e.g. policies, forms, action plans, links to documents or websites)

Details of the data items are provided in Appendix 1 - Assertions and evidence items . Details of timescales are provided in section 10.

14. Helpdesk

Users should raise all incidents and support requests with the DSP Toolkit helpdesk. Support requests can be raised by telephone (9.00 – 17.00 on weekdays) or by email. Contact details are available from the help menu of the DSP Toolkit: https://www.dsptoolkit.nhs.uk/ .

Target service levels for the helpdesk (and service availability) are summarised below:

Description	Target
Total supported service availability (excluding planned downtime)	98%
Period of planned downtime	Maximum of 10 working days per annum
Restoration of full production service to failover infrastructure	Within 4 hours

All incidents are dealt with in order of priority allocation, with 1 being the highest order of priority. Incident categorisations, and target resolution timescales are as detailed in the table below:

Service Impact (see following table)	Overall % Target	Priority Derived	Response Within	Resolution Within
High	99%	1	2 hours	3 working days
Significant	95%	2	4 hours	6 working days
Medium	95%	3	No target	10 working days
Low / None	95%	4	No target	As agreed

An incident or support request may pass from 1st to 2nd to 3rd line support teams within these timescales. From a user's perspective it is one incident or support request raised and dealt with in the timescales outlined.

Appendix 1 - Assertions and evidence items

This is made available as a separate document on the NHS Digital website:

http://digital.nhs.uk/isce/publication/dcb0086