Document filename:	Data Protection Impact Assessment – Data Security and Protection Toolkit (DSPT)	
Directorate / Programme	Data Security Centre - Data Security and Protection Toolkit	
Document Reference	IAR0000390	
Information Asset Owner	Alan Morton	Version 3.1
Author	David Ingham / John Hodson	Version issue date 23/07/2020

Data Protection Impact Assessment – Data Security and Protection Toolkit

Document Management

Revision History

Version	Date	Summary of Changes
1.1	16/08/2019	First draft (revised template)
1.2	26/08/2019	Updated draft (following feedback)
2.0	20/09/2019	Updated draft (following feedback)
3.0	21/10/2019	Updated draft (following feedback)
3.1	23/07/2020	Updated draft (following feedback)

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
Alan Morton	Information Asset Owner	23/07/2020	3.1

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document 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.

Contents

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS Digital demonstrate how we comply with data protection law.

DPIAs are also a legal requirement where the processing of personal data is *"likely to result in a high risk to the rights and freedoms of individuals".* If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire

1. Consultation with Stakeholders

In 2015 over 1000 users responded to a survey regarding the existing IG toolkit. These comments and the findings of the NDG review have informed the development of DSPT.

Prior to launch, a prototype system was tested by over 250 users in health and social care.

Since November 2017 over 800 individuals have attended workshops across the country. This has entailed demonstrations of the system, feedback on its ease of use and a chance for assumptions to be tested through user research workshops.

In addition, over 3000 participants have joined online webinars including a system demonstration and Q&A session.

Users of the system are able to provide feedback through an online form. These comments are reviewed on a weekly basis. Over 1000 pieces of feedback have been provided (75% of which has been positive).

Consultation has been carried out with;

- NHS Digital Data Security Centre, Live Services Exeter, Exeter Digital Delivery Centre
- Department of Health and Social Care / NHSX
- NHS England and Improvement
- The Information Commissioner's Office
- Office of the National Data Guardian
- The Care Provider Alliance
- Key User Groups E.g. Strategic Information Governance Network

57 user research events have taken place to obtain feedback from users on a 1 to 1 basis. All these events / methods have shaped the ongoing development of the DSPT. The Government Digital Service have assessed the approach to user research and provided positive feedback.

2. Data Flow Diagram

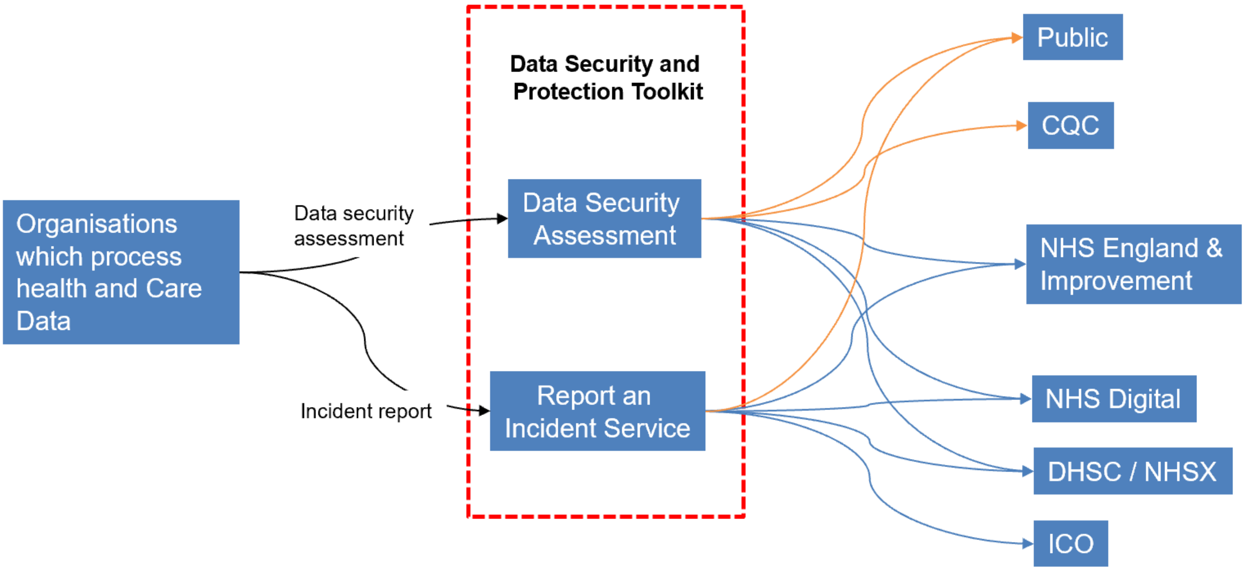
Data Flows

Organisations record self-assessment information on the Data Security and Protection Toolkit, which is then made available to NHS Digital, the Department of Health and Social Care / NHSX, NHS England & Improvement. Aggregated reports and an overview of toolkit status is available to the public and the Care Quality Commission.

Incident reporting information is made available to the ICO, NHS Digital, NHS England/Improvement and the Department of Health and Social Care / NHSX. Aggregate information pertaining to reported incidents is also made available to the public at https://www.dsptoolkit.nhs.uk/News/63.

This publication details the number of incidents reported to the ICO broken down by sector, the number of incidents where the "Likelihood that citizens' rights have been affected" is reported as: "likely" "highly likely" or "occurred", the number of incidents reported with a potential adverse effect, and the number of incidents reported as being caused by a problem with a network or information system.

Please see the diagram below:


Organisations which process health and Care Data
Data security assessment
Incident report
Data Security and Protection Toolkit
Data Security Assessment
Report an Incident Service
Public
CQC
NHS England & Improvement
NHS Digital
DHSC / NHSX
ICO

Key:
Orange line = aggregated reports

Blue Line = detailed information

3. Purpose of the processing

The DSPT was developed in response to the National Data Guardian “Review of Data Security Consent and Opt Outs” July 2016 and Government Response “Your Data: Better Security, Better Choice, Better Care” July 2017.

The purpose of the DSPT is:

(i) For organisations to demonstrate to relevant national and local bodies their compliance with mandated standards for data protection, data security, and cyber security;

(ii) (ii) To allow organisations to understand the data protection and security risks to their data and essential services, including in comparison to other, similar organisations;

(iii) (iii) To enable national and regional bodies to understand data protection and security risk to data and essential services across the health and care system and determine appropriate responses and interventions;

(iv) (iv) To give the public confidence in how health and care organisations handle some of their most sensitive personal data.

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.

The ultimate aim is to demonstrate that the organisation 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 data.

This will minimise the number of individuals who 'opt out' of the sharing of their personal identifiable data. Using the toolkit to perform a self-assessment against the standard will allow organisations to identify and implement action to address any shortcomings, which in turn will reduce the organisation’s risk of a data breach.

4. Description of the Processing

Nature and scope of the processing:

The DSPT is completed by organisations that process health and care data – this includes:

Acute Trusts, Ambulance Trusts, Community Services Provider, Mental Health Trust, Arms Length Bodies, CCG, CSUs, NHS Digital, AQP Clinical Services, AQP Non Clinical Services, Care Homes, Charities/Hospices, Companies, Dentists(NHS), Dentists (Private), Domiciliary Care Organisations, Local Authorities, NHS Business Partners, Opticians, Pharmacies, Prisons, Researchers, Secondary Use Organisations, Universities and GPs.

The system comprises:

1. Self-Assessment: The ability for a health or social care organisation to measure its performance against legal requirements and central guidance to demonstrate information is handled correctly and protected from unauthorised access, loss, damage and destruction.

As part of this assessment the name, email address and telephone number of key roles (only) within each organisation are requested. No special categories of personal data are requested. Limited incidental personal information may be held where organisations have recorded this in their submissions. The personal information included as part of the assessment is only shared with a small number of organisations including NHS Digital, the Department of Health and Social Care / NHSX, NHS England & Improvement.

A summary of the Data Security and Protection Toolkit self-assessment is published via the DSP Toolkit website.

2. Report an incident: The DSPT provides the ability for a health or social care organisation to record and report the details of a data security and protection incident that breaches the General Data Protection Regulation / Data Protection Act 2018 to the Information Commissioner's Office (ICO) electronically. This also discharges the contractual and policy responsibility to report to NHS Digital, NHS England/Improvement and the Department of Health and Social Care simultaneously. For applicable organisations (Acute, Mental Health and Ambulance Trusts) this will allow them to report any breaches of Network and Information (NIS) Services Directive to the competent authority which is the Department of Health and Social Care. No special categories of personal data are requested.

Context of the processing:

NHS Digital is the data controller for this processing. 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 are required to carry out self-assessments of their compliance against the assertions and evidence items contained within the DSP Toolkit and use the DSPT to notify regulators of Data Security Incidents.

Circa 27,500 toolkit assessments are published each year containing approximately 41,000 records of name, email address and telephone number. Processing is usually English data but will occasionally be for individuals from United Kingdom, Europe or the rest of the world. Organisations typically update details once per year but can updated at any time during the year. Organisations can edit at any time and able to view results internally confirmed once per year

Storage and Disposal

Each submission to the DSPT and related evidence is stored by NHS Digital. The DSP Toolkit is available to all users (whether through n3/HSCN or public internet) via a www domain: www.dsptoolkit.nhs.uk

Data is stored in England and Ireland. Data will be disposed of in accordance with the NHS Digital Platforms and Infrastructure Media Disposal and Data Destruction Process.

5. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?

For the DSPT self-assessment

Legal basis for collection:

A Direction given by the Secretary of State for Health requiring NHS Digital to establish and operate a system to be known as the data security and protection toolkit data collections service.

Direction -(s.254 (1), (2)(a), (5) and (6), and 260(2)(d) of Health & Social Care Act 2012)

For the small amount of personal data the legal basis is Article 6 of the GDPR for the processing of personal data (Article 6 (1c) – *processing is necessary for compliance with a legal obligation to which the controller is subject*). This will be shared with NHS Digital, the Department of Health and Social Care / NHSX, NHS England & Improvement

Legal basis for analysis:

Direction - sections 254(1), (2)(a), (5) and (6), and 260(2)(d) of the Health and Social Care Act 2012.

Legal basis for disclosure:

In accordance with section 260(2)(d) of the Act, NHS Digital is directed not to publish the data obtained by complying with the section 254 Direction except for a summary level of each organisation's completed data security and protection toolkit which will be made available online to the public.

Direction located at:

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

For Incident Reporting:

Legal basis for collection:

Under sections 254(1) (6), 260 (1) and 2(d) of the Health and Social Care Act 2012 and 304 (9) (10) and (12) of the Health and Social Care Act 2012.

For the small amount of personal data the legal basis is Article 6 of the GDPR for the processing of personal data (Article 6 (1c) – *processing is necessary for compliance with a legal obligation to which the controller is subject*). This may be shared with the ICO, NHS Digital, NHS England/Improvement and the Department of Health and Social Care / NHSX.

Legal basis for analysis:

Under sections 254(1) (6), 260 (1) and 2(d) of the Health and Social Care Act 2012 and 304 (9) (10) and (12) of the Health and Social Care Act 2012.

Legal basis for disclosure:

In accordance with section 260(2)(d) of the Act, NHS Digital is directed not to publish the data obtained by complying with the section 254 Direction except for a summary level of each organisation's completed data security and protection toolkit which will be made available online to the public.

Direction located at:

https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/data-security-and-protection-incident-reporting-tool-direction-2018

6. Demonstrate the fairness of the processing

Data is submitted to the DSPT by all organisations that have access to patient data. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly, as determined by DHSC.

Limited incidental personal information may be submitted where organisations have recorded information in their submissions. An individual may not expect their personal information to be processed in this way, but we believe the risk of this is slight, and the potential processing of this information is necessary, fair and proportionate to achieving the aim that organisations demonstrate that they can be trusted with the confidentiality and security of personal information.

The personal data specifically requested by the system is the details required for controlling users' access to the systems and details of key staff with responsibility for data security. Any personal information processed outside of that requested will not lead to unjustified adverse/detrimental effects on individuals.

Details of how the information recorded on the DSPT is used is made available to users through the Privacy Policy the Legal Directions (see section 5) and through publication of this DPIA on the DSPT website.

7. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

NHS Digital has no direct relationship with individuals who may have information about them submitted to the DSPT. Details of why NHS Digital collects this information, how the information recorded on the DSPT is used and how individuals can assert their rights over this data is made available to users through the Privacy Policy the Legal Directions (see links at section 5, above) and through publication of this DPIA on the DSPT website.

Our Privacy policy states that we strive to capture a minimal amount of personal data and only share it with other organisations where the law permits us to do so.

The DSPT is noted within the NHS Digital Corporate Transparency notice:

https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register

8. Is it necessary to collect and process all data items?

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
Personal Data		
Name	Yes	The names of key roles are required to identify who is accountable for data security within an organisation. The names of registered users are required to identify who is providing information.
Address	N/A	
Postcode	N/A	
DOB	N/A	
Age	N/A	
Sex	N/A	
Marital Status	N/A	
Gender	N/A	
Living Habits	N/A	
Professional Training / Awards / Education	N/A	
Income / Financial / Tax situation / Financial affairs	N/A	
Email Address	Yes	Contact information for key roles is also held in the event NHS Digital needs to contact the relevant accountable individual. Registered users' contact information is held in the event NHS Digital or regulators need to contact the relevant user, including automated messages such as password resets and confirmation emails.
Physical Description	N/A	
General Identifier e.g. NHS No	N/A	
Home Phone Number	N/A	
Online Identifier e.g. IP Address/Event Logs	Yes	IP addresses are stored in "login" logs by the Toolkit for error tracking and security purposes. IPs are useful for identifying errors caused by somebody being logged in on the same account at a different location. They are also useful for identifying malicious requests and where they were coming

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
		from.
Website Cookies	Yes	We use session cookies to authenticate a user login, to allow access to authorised functions within the site and to enhance navigation of the site during the user's session. Specific details are provided at: https://www.dsptoolkit.nhs.uk/Home/Privacy
Mobile Phone / Device No / IMEI No	Yes	Contact information for key roles is also held in the event NHS Digital or regulators need to contact the relevant accountable individual. Registered users' contact information is held in the event NHS Digital needs to contact the relevant user.
Location Data (Travel / GPS / GSM Data)	N/A	
Device MAC Address (Wireless Network Interface)	N/A	
Banking information e.g. account number, sort code, card information	N/A	
Criminal convictions / alleged offences / outcomes / proceedings / sentences	N/A	
Spare – add data item (as necessary)		
Spare – add data item (as necessary)		
Special Category Data		
Physical / Mental Health or Condition	N/A	
Sexual Life / Orientation	N/A	
Religion or Other Beliefs	N/A	
Trade Union membership	N/A	
Racial / Ethnic Origin	N/A	
Biometric Data (Fingerprints / Facial Recognition)	N/A	
Genetic Data	N/A	

9. Describe if personal datasets are to be matched, combined or linked with other datasets? (internally or for external customers)

No

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

Contact information is shared with regulators where incidents are reported through the DSPT.

Contact information for those individuals with key roles may be shared with regulators so that this information may be cross referenced to identify discrepancies and ensure data quality (i.e. to ensure email address information is accurate).

When required, and by virtue of the Direction, NHS Digital may share copies of DSPT submissions with DHSC, NHSE/I, ICO.

11. How long will the personal data be retained?

Data will be retained for a maximum 12 years before being deleted and disposed of securely. This is for trend analysis and standard practice for the Data Security and Protection toolkit and the Information Governance Toolkit has been to retain information submitted through the DSPT for seven years

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

The personal data collected is that which is provided by users in order to manage their organisations DSPT assessment i.e. users, administrators, key roles which they are under an obligation to keep up to date themselves.

If requested, local administrators and members of the DSPT team can delete users access i.e. when an administrator has left an organisation and has not deleted their own account details.

Data validation is in place to ensure telephone numbers and email addresses are correctly formatted.

Submissions to the DSPT may inadvertently contain personal data, and these submissions are stored by NHS Digital. Where submissions are used to support an application for patient data through the Data Access and Request Service, the published submission from that year is used. NHS Digital does not and is under no obligation to request an update from the organisation in question.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

Information is provided on the DSPT website and privacy policy including details of how to request a copy of personal information held by NHS Digital.

As NHS Digital are processing the data under a legal obligation, the rights available for individuals to exercise are as follows:

- Right to be informed
- Right of access
- Right to rectification
- Right to restrict processing – where an individual contests the accuracy of the personal data, processing should be restricted until accuracy has been verified

Rights requests will be dealt with in line with NHS Digital's policies and processes.

14. What technical and organisational controls for "information security" have been put in place?

A System Level Security Policy (SLSP) ref: SLSP0000040 is available from the Unified Register. This includes further detail including access control, encryption, hosting and penetration testing. The SLSP is a document created by the System Owner to show a concise and considered view of the information security of a system at any given time. It demonstrates understanding of information security risks and commitment to address the confidentiality, integrity and availability of the system.

Further organisational controls include the following reminder to users when submitting an incident report:

Please ensure there is no personal data included in the details of the incident

And then confirmation checkbox (which the user must proactively tick) which says:

I confirm that no personal information (including name or contact details of individuals responsible for the incident or informed about the incident) has been provided in this incident report.

15. In which country/territory will personal data be stored or processed?

England and Ireland.

16. Does the National Data Opt Out apply to the processing?

No

17. Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Alan Morton 23/07/2020