Process for projects using the Data Security and Protection Toolkit (DSPT) as the security assurance

This version (v3.1) approved by the IG Committee 2023-07-25

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows an organisation to measure their performance against the National Data Guardian's 10 data security standards. The IG Committee assesses our policies and processes against this tool annually in order to provide assurance that members of the Division of Population Health practise good data security and that personal information is handled correctly.

Anyone that wishes to use Division of Population Health's NHS DSPT submission as the security assurance for their project (e.g. projects using NHS England Data, data obtained using CAG / Section 251 approval) must be a staff member within the Division of Population Health and meet the criteria of Information Asset Owner (IAO) policy, typically either: the Principal Investigator (PI) for the project; or, a work-package lead. As such they must comply with the rigorous set of information security standards set out within the DSPT assessment.

The IG spot checks procedure will be followed when a member of the IG Committee is contacted regarding the potential to use the NHS DSPT as the security assurance.

The IAO using the Division of Population Health's NHS DSPT as the security assurance, must comply with the following actions:

Notify the IG team

Inform the IG committee (either the IG manager or section IG lead) about any project that uses the DSPT as the security assurance, ideally prior to beginning the application process (for NHS England data, this means prior to beginning the Data Access Request Service (DARS) application process); but certainly before getting a signed off Data Sharing Agreement (DSA). See https://www.sheffield.ac.uk/scharr/division-population-health-information-governance-policy/information-governance/scharr-information-governance-committee

All DSPT assured projects must be included on the Division of Population Health's DSPT as a security assurance asset register. The IG manager or section IG lead will liaise with the project team to collect the necessary information to populate the asset register, as per the IG spot checks procedure.

Adhere to IG Policies and processes

Read and ensure compliance with the IG policy
Read and ensure compliance with Information Asset Owner (IAO) for Division of Population Health projects

Do the necessary training

The IAO must ensure that any individual who will access DSPT assured data has a staff contract, is a UoS student, or has an honorary or secondment contract with the University of Sheffield which contains as standard appropriate terms about data security and data protection. All individuals who will access DSPT data must have a valid record of completion for all mandated training modules throughout the period of their access to the data:

- UoS Protecting Information
- UoS Protecting Personal Data
- UoS Protecting Research Data
- UoS Cyber Safety
- Any relevant UoS SDS Training (where a requirement to use this service has been identified in the data management plan)
- Division of Population Health Information Governance

These can be found here: https://infosecurity.shef.ac.uk/

For NHS England data only: Read the Data Sharing Framework Contract (DSFC) (link here)

All personnel, prior to accessing or using NHS England data, must be fully aware of, and comply with the terms and conditions set out in the DSFC and the relevant DSA.

Some notable terms are:

- The data recipient must not disseminate the data further unless NHS England has specifically authorised this.
- The data must only be used in accordance with the express terms of the DSFC and DSA and for only the purpose(s) outlined in the DSA.
- Results / aggregate data derived from the NHS England data may only be shared outside of the immediate project team if it (a) cannot be identified as originating or deriving from the Data and cannot be reverse-engineered such that it can be so identified; and (b) is not capable of use as a substitute for the Data; and (c) has not at any time been verified by NHS Digital as not fulfilling the criteria (a) and (b) above .

However, it is important that members of the Division of Population Health accessing data are aware of all terms.

Ensure the Data Sharing Agreement is signed by Research Services

All Data Sharing Agreements (for any project, not just NHS England projects) **must** be signed on behalf of the University by Research Services (email ri-contracts@sheffield.ac.uk).

For NHS England projects the University of Sheffield authorised signatory named in the DARS application must be the Director of Research Services (using the central email of ri-contracts@sheffield.ac.uk; currently Deborah Lodge is the signatory). This will ensure that the DSA will be routed correctly through the NHS England online approval portal to Research Services for sign off.

Please also send a copy to the IG manager or section IG lead notifying them that it is ready for sign off.

All personnel, prior to accessing or using shared data, must be fully aware of, and comply with the terms and conditions set out in the relevant DSA.

See also Section 5 (Information Sharing) of the IG policy.

Set up your privacy notice (if required)

NHS England require a privacy notice for all studies, other data providers may also require this depending upon the type of data provided and regulatory approvals; if you are receiving personal data a Data Protection Impact Assessment (DPIA) or equivalent should be conducted (NB the University Research Ethics Committee (UREC) agreed that obtaining ethics approval is evidence of a staff procedure for carrying out a DPIA, however there may be cases where an additional DPIA is required). The interpretation of the legislation by NHS England is that they are processing personal data on behalf of the study, and therefore the study should have a privacy notice in order to meet the legal obligation to inform individuals. There is more information regarding the right to be informed on the ICO website. Please contact the IG team for advice on how to set up your privacy notice. It's expected that the majority of the time the privacy notice will be included on a study specific webpage, usually on The University of Sheffield's website. Following the merger of NHS Digital with NHS England, should your privacy notices mention NHS Digital, you should change those references to NHS England at the next update.

Request data storage and computing resources that are compliant

All projects that provide the Division of Population Health's Data Security and Protection Toolkit as the security assurance are advised that users access this data using managed

machines and secure storage (as outlined in Section 3 (Data Storage and Storage Devices) of the IG policy) or the Secure Data Service (SDS) where a requirement to use the service has been identified in the data management plan. This is to ensure compliance with the responses in the Division of Population Health's DSPT regarding encryption, antivirus and antimalware updates, patch management, supported software and software updates.

Access to data should only be granted to those individuals who require access and comply with all aspects of the DSPT.

By default, data processing for all DSPT projects should be undertaken on an access restricted folder on the University's Shared Networked Filestore (X drive), a UoS research virtual machine (VM) or on the SDS. Where this is not practical, alternative or additional secure data storage must be chosen based on an assessment of potential risk. Advice must be sought from the relevant Section IG Lead..

Requests for an access restricted folder on the X drive should go to the Division of Population Health DS.

When using the SDS, data should be stored within the project environment provided to you, and nowhere else.

DSPT assured data must never be stored anywhere other than in the access restricted project folder on the University's Shared Networked Filestore ("X drive" folder), the University networked filestore allocated to the VM (though it is recommended that the access restricted X drive folder is still the data repository if processed via a VM), or on storage provided on the SDS).

Google Drive should **never** be used for DSPT assured data.

See also Section 3 (Data Storage and Storage Devices) of the IG policy.

It is not expected that there will be any paper copies of risk-bearing data, if there are reasons this is necessary the arrangements for keeping this paper secure must be documented and paper records must not be removed from UoS premises.

Notify the IG team of any changes

Any changes to the data sharing agreement or to the project team who have access to the data must be notified to either the IG manager or section IG lead.
Anyone who has access to the data must be compliant with the processes above.

Destroy data

Destroy datasets when they are no longer needed or when permission to hold them expires (whichever is the sooner); as per the data destruction process.

It may be possible to retain appropriately anonymised or derived data (as allowed under the contracts governing the data sharing), along with analysis code and data extraction requests. However, details of retained data should be declared and agreed as appropriate with the data provider. This may also need documenting within the data destruction certificate.

Under no circumstances shall the Data Recipient retain the Data without an extant DSA and Contract (or New Contract) in place which relates to that Data.

Ensure contractual compliance when publishing results

Ensure that any agreements regarding publishing and dissemination and terms within contracts, i.e. the Data Sharing Framework Contract (DSFC) for NHS England projects are adhered to. This may be, for example, an agreement to suppress small numbers (typically 1 - 7 [inclusive] and all other numbers rounded to nearest 5)[1] in any quantitative reporting, an agreement to acknowledge the data source, or an agreement to confirm with NHS England that any “derived data” are sufficiently derived as to be no longer sensitive.
NHS England state If you are publishing outputs that arise from the data then you should quote the following:
'This work uses data provided by patients and collected by the NHS as part of their care and support.’

If there is a data security incident, follow the incident policy

If you discover that data security may be at risk, follow the instructions within Section 6 (Incident Management) of the IG policy.

Version	Effective Date	Summary of changes
1.0	25-May-2021	n/a first version
2.0	24-Jan-2022	Updated to include the DSH
3.0	30-Mar-2023	On 1 February 2023, NHS Digital merged with NHS England. NHS England assumes responsibility for all activities previously undertaken by NHS Digital. Cyber Essentials Plus may no longer be supported by Central University. Honorary T&Cs must include terms regarding data security and protection. Requirement to update

[1] Refer to the latest version of the HES Analysis Guide’s rules on Disclosure Control

		reference to NHS digital in privacy notices at the next update. Change to reflect re-branding of Data Safe Haven to Secure Data Service. Updated to remove references to the Assured Computing platform.
3.1	25-Jul-2023	Preference for use of an access restricted folder on the X drive, rather than VM reflected. Information regarding paper records added. Further clarification of statistical disclosure control added.