Spot check procedure v4.0

This version (v4.0) approved by the IG Committee 2023-05-30

Background

In order to ensure staff understand and comply with procedures that ensure the security assurances outlined in the ScHARR Data Security and Protection Toolkit (DSPT) are met a number of checks are carried out. Maintenance of the DSPT as security assurance asset register (asset register) is crucial in ensuring and documenting that these checks have been carried out.

Our ScHARR Information Governance policy training states that the Section IG Lead must be informed of any projects using personal data from a third-party provider (e.g. NHS England) and ScHARR staff are reminded at intervals of this.

Purpose

This procedure outlines the steps involved in ensuring checks are carried out and maintaining the asset register, as well as who is responsible for this and when these steps occur.

Scope

Any project that uses the ScHARR DSPT as a security assurance must be listed on the asset register.

Procedure

New studies

The ScHARR IG Manager is made aware of a project using data from a third-party provider where the DSPT is required as a security assurance. Either the researcher contacts the ScHARR IG Manager directly, or the ScHARR IG Manager is informed via the Section IG Lead, a member of the Contracts Team in Research Services or because the project appears on the NHS England Data Use Register.

The ScHARR IG Manager reviews any initial documentation provided and, as long as there are no inaccuracies regarding any of the data protection or security assurance information, provides the researcher with the DSPT information. The researcher is reminded that:

- they must provide information for the asset register when requested
- they must keep the ScHARR IG Manager updated of any changes
- any data sharing agreement(s) must include details of all third-party data processors and data centres where applicable and requested
- they must ensure any data sharing agreement(s) are signed off by a member of the contracts team in research services (ri-contracts@sheffield.ac.uk)
- should be familiar with the Process for projects using the DSPT as the security assurance

- (if involving NHS England data) they must read the data sharing framework contract (DSFC)
- they must assign an Information Asset Owner (IAO) who must abide by the Information Asset Owner policy
- The IAO
    - takes on the responsibility to keep the ScHARR IG Manager updated regarding any changes, including access, and with updated information.
    - must use data storage and computing resources that are compliant with ScHARR IG policy and/or the Secure Data Service (SDS) where a requirement to use the service has been identified in the data management plan
    - should document any spot checks if carried out
    - must read the Process for projects using the DSPT as the security assurance
    - (if involving NHS England data) they must read the data sharing framework contract (DSFC)
- anyone who will access the data
    - must read the ScHARR IG Policy
    - must have up to date training
    - must only access and process the data within the data storage assigned (i.e. they must not move or copy the data)
    - if they use a mobile device for work purposes (e.g. accessing emails etc) it must be encrypted
    - (if involving NHS England data) they should be familiar with the data sharing framework contract (DSFC)
    - they should read the Process for projects using the DSPT as the security assurance.

This may be a face to face meeting, if the researcher wishes, or communicated via email.

The ScHARR IG Manager adds the data source, title and project lead to the 'In progress' tab of the asset register.

Ongoing

Ad hoc checks

The asset register is reviewed regularly by the ScHARR IG Manager for gaps and researchers are reminded to provide the following

Updates expected from researcher	Required action by ScHARR IG Manager (all folders are in ScHARR Information Governance > Asset register / Data Sharing agreements)
Provides draft DSA	Review for compliance, ensure contracts team are involved in sign off. Ensure all third party data processors and data centres are listed (if applicable).

	Request approved version once signed off. Request data flow and DMP if not also provided
Provides signed DSA	Save to 'Copies of project DSAs' folder and link to asset register, update date from and date to columns. Request data flow and DMP if not also provided. Check there are no conditions to approval, e.g. privacy notice approval and follow up if there are any.
Provides data flow and DMP	Review for compliance, save to 'Data flows' and 'DMP' folders and link to asset register. Remind researcher to let IG Manager know when data is received, request details of arrangements for data storage, what software is planned to be used and details of who (including user id) will have access
Planned data storage, software and data access information provided	Review for compliance. Update details of data location (including VM path and name if applicable), software, desktop and people who have access. Add to / check staff with access to data to the tab in the asset register and ensure their training is up to date and they have confirmed they understand that their system use can be monitored and recorded
Data has been received	Ask for an update on who has access and check arrangements for data storage and access have not changed.
Notified of access changes	Update people who have access and update staff with access to data to the tab in the asset register; carry out the necessary checks
Destruction certificate provided	Save to 'Destruction certificates'. Move record to destroyed tab of asset register and link to asset register.

Regular review of the asset register

Review DSA end dates on the asset register and follow up with researchers regarding any due to expire within the next month. Review any outstanding spot check issues and follow up with researchers.

Annual checks

NHS England publishes the NHS England Data Use Register. The published DSAs must be reconciled with the asset register. Any anomalies should be followed up internally initially (with research services and SDS group); data.applications@nhsdigital.nhs.uk must be contacted if there are any DSAs we do not recognise.

In addition, also review access to data locations with ScHARR-DS (for X drive folders), IT Services (for VMs), or the SDS team (for the SDS); ensure access logs match the asset register. Check with researchers that those with access still require

access. Ensure all training is up to date. Check data storage locations are still correct and up to date.

Spot check log

In addition to keeping the asset register up to date, keep a log of questions / issues raised with who and on what date as a reminder of what issues are ongoing and their status.

Version	Effective Date	Summary of changes
1.0	20-Feb-2020	n/a first version
2.0	25-May-2021	Addition of mobile device status check; DSPT as a security assurance process and IAO policy.
3.0	24-Jan-2022	Added References to the Data Safe Haven
4.0	30-May-2023	Added prompts about data storage and data processing locations. NHS Digital is now NHS England. NHS England will no longer provide a report, therefore this process has changed and requires review of the Data Use Register. Data Safe Haven is now Secure Data Service. Cyber Essentials is no longer applicable. Added a recommendation that staff document any spot checks if they carry them out themselves. Added some clarity around requirement for the researcher completing the application for data, the IAO and staff who will have access to data.