MANCHESTER 1824

The University of Manchester

Standard Operating Procedure

Number:	UM/17/SOP/NHSIGTK004		
Title:	The Data Safe Haven		
Version:	2.0	**Effective Date**	27/09/2018
Author:	Diane Escott	**Review Date**	As required
Reviewed by : April Lockyer		**Approved By:** Nalin Thakker	
Position: Head of Research Governance, Ethics and Integrity		**Position:** Associate Vice President for Compliance, Risk & Research Integrity	
Signature: 		**Signature:** 	

Version	Date	Reason for change
2	27/09/2018	To align with the DSH SLSP

When using this document please ensure that the version you are using is the most up to date either by checking on the Directorate of Research and Business Engagement Support Services website (http://www.staffnet.manchester.ac.uk/services/rbess/governance/compliance/policiesandprocedures/) for any new versions or contacting the author to confirm the current version.

1 Background

The Data Safe Haven provides an infrastructure for the secure management and processing of highly restricted data that is personal, sensitive and confidential in nature. It is a repository for data for the following types of studies:

- All NHS-Digital data users who need to be NHS Information Governance Toolkit (IGTK) compliant, unless there are reasons this cannot proceed.
- Other, non NHS-Digital data users who also need to be NHS IGTK compliant, including section 251 approval.
- Other, non NHS-Digital data users where the data is highly sensitive and their security requirements could only be met by a data safe haven.
- Defence data

The Data Safe Haven enables the University to demonstrate that the data for such studies will be stored and used within a secure environment as part of the compliance obligations. Access to the Data Safe Haven is restricted to on-campus connectivity only. For data that meet the above criteria, but which cannot be stored in the safe haven, procedures within the SOP for 'Information Security Classification, Ownership and Secure Information Handling' must be followed. http://documents.manchester.ac.uk/display.aspx?DocID=29971

2 Purpose

This Standard Operating Procedure (SOP) describes the process by which projects in receipt of data that meet the criteria described in (1) can manage their data within the University of Manchester's Data Safe Haven.

3 Roles and Responsibilities

Role Definitions

Information Governance Lead for the Data Safe Haven

The Head of Research Governance, Ethics and Integrity is the Information Governance Lead for the Data Safe Haven. It is his/her responsibility, supported by a Research Governance, Ethics

and Integrity Officer, to put appropriate policies and procedures in place to ensure the security of the data stored within the Data Safe Haven.

The IG Lead for the Data Safe Haven is responsible to the University's Research Compliance Committee (RCC) and will submit, on a quarterly basis, a report to RCC that will include non-conformances and lessons learned to improve this procedure.

Oversight of the Data Safe Haven is maintained by the Data Safe Haven Operations Group which meets every two months and is chaired by the Information Governance Lead for the Data Safe Haven.

Principal Investigator (PI)

The PI takes responsibility for the safekeeping of the data in accordance with any contractual arrangements with the data provider, with good research practice and the policies and procedures of the University of Manchester (the University). These duties are outlined in the Investigator Agreement, which must be signed by the PI before s/he can use the Data Safe Haven. In this Investigator Agreement the PI is the Information Governance Lead for the study, even if s/he has delegated duties to a nominated Study IG Lead. The PI must have the necessary and suitable experience and expertise to design, conduct and report the study to standards expected by the data providing organisation such as NHS Digital, and all legal and ethical requirements. In addition, they must comply with the University of Manchester Policies and SOPs, and the SOPs of any NHS Trusts, if appropriate.

The PI is responsible for ensuring that this document is observed in respect of the data for which they have responsibility. This includes, making all staff that access and use the data aware of this document. The University expects all persons operating on University sites to comply with the policies and any subsequent amendments and to seek to comply with all Codes of Practice issued by NHS Digital and other data providers where their security requirements entail use of a data safe haven and relevant University wide and/or local Standard Operating Procedures (SOPs).

Staff awareness of this Procedure will be audited periodically by the Research Governance, Ethics and Integrity Officer.

The PI is accountable to the IG Lead for the Data Safe Haven and will report on compliance on a quarterly basis.

Study Information Governance Lead (SIGL)

The PI may nominate a Study IG Lead to carry out, on their behalf, the duties outlined in the Investigator Agreement.

Research IT

IT support for the DSH will be provided by Research IT.

4 Procedure

4.1 Requesting use of the DSH

The Data Safe Haven can only be used on campus and with the permission of the IG Lead for the Data Safe Haven. The following procedure must be followed by all UoM employees who require use of the DSH, including requests by supervisors for the storage of data for student projects. Requests will not be accepted from students or non-UoM employees. The procedure is as follows:

a. The researcher should complete a Data Management Plan which flags up the requirement for usage of the DSH to the Research Governance, Ethics and Integrity team (RGEIT).

b. Researchers are then expected to complete a request for use of the DSH to Research IT via the appropriate Data Safe Haven Landesk Form (found under Research IT Services). [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=5eddb060-e22f-4654-a024-42ed9d761e22]. On receipt, Research IT will forward a copy of the Landesk form to the RGEIT.

c. The RGEIT will collect the following details from the Landesk form:
   - Identity of the PI and username
   - Identity of the Study IG Lead and username
   - Identity of all users, including username
   - Name of the project
   - And other such information around Information Governance and service requirements

4.2 Approving user access to the DSH

Before approving use of the DSH, the following conditions must be met for all users:

a. Completion of the University's Data Protection Training.
b. A data sharing contract must be in place between the UoM and the data provider which confirms authorised users and the specific data they are entitled to access. This must be checked by the RGEIT.
c. An SLSP written by Research IT with the PI, based on the requirements of the data provider and detailing those users who require access to the data.
d. An Information Governance Risk Review will need to be completed by the PI and submitted to the Information Governance Office for review.
e. An IG master file will need to be developed which outlines the quality assurance processes that must be put in place in order to use the DSH. This will be overseen by RGEIT.
f. An Investigator Agreement signed by the PI which states the responsibilities of the PI and the Study IG Lead, where appropriate. This will be overseen by RGEIT.

Only when these conditions are met will RGEIT request Research IT to take the required steps to provision users and projects into the DSH. It is understood that data users may work on more than one project and therefore require access to different project folders in the DSH. In this instance, users will only be provided access to the project folder for which all the above conditions are met. Access to one project will not automatically grant access to other projects. In addition, the same process will apply to external collaborators who require access to a project folder.

Research IT will notify the RGEIT and the users when they have been granted access to the DSH by copying in RGEIT to all emails issued to DSH users.

4.3 Transferring your data into the DSH

The first step in transferring data into the DSH will be for you to download the data to a single point within the University of Manchester so as to reduce the data footprint in alignment with the requirements of third party data providers, such as NHG Digital, and provide evidence should an audit take place. The single point is provided via a static IP addressed laptop within the RGEIT offices. The download must be carried out by the PI or Study IG Lead within the research group who holds permission to do this, as already set up by Research IT during the DSH request process.

4.3.1 Once the PI or Study IG Lead have been granted access to the DSH by Research IT, they will then contact the RGEIT to book an appointment to access the laptop in order to transfer the data from the data provider into their space in the DSH.

> *Please note that in order to use the Secure Transfer Service, the PI or Study IG Lead will need to use the University's 2-factor authentication Service (Duo) to verify their identity before they can gain access. To register with Duo, the PI or Study IG Lead should visit the IT Account Manager site (click the **Sign in to IT Account Manager** button and then click the **2FA(DUO)** tab) and then follow the registration instructions.*

4.3.2 The PI or Study IG Lead will log into the laptop using their UoM username and password, followed by the 2FA procedure.

4.3.3 The PI or Study IG Lead once logged into the laptop can follow the instructions from the data provider on how to download the data. The data should be downloaded onto the local hard drive of the laptop (c:\work) and not onto the user's desk top area (this is your p-drive).

4.3.4 Once the data is downloaded onto the laptop, the PI or Study IG Lead will then upload the data from the c drive of the laptop into the data safe haven using the Secure Transfer Service, please follow the instructions below.

Instructions for using the Secure Transfer Service:

4.3.4.1 Go to https://filetransfer.dsh.manchester.ac.uk.

4.3.4.2 Enter your **University login details** into the login screen.

4.3.4.3 A passcode prompt will appear.

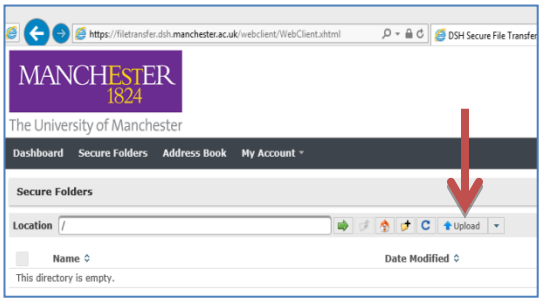
4.3.4.4 Select an **authentication option**. Enter the **number** into the empty field and click **Submit**.

Option	Number
Duo Push (smartphone)	1
Phone call	2
SMS passcode (SMS text message)	3
Duo key fob	Enter the code you received

4.3.4.5 If using the phone call or SMS options, enter the **code** you received into the empty field.

4.3.4.6 When you have successfully logged into the Secure Transfer Service, you will be presented with the file transfer portal. Browse the laptop and select the **file** you want to upload within the c:\work folder.

Click the **Upload** button. The file will then be transferred into the DSH. Uploaded files will be listed in your project folder when they have been successfully transferred.



4.3.4.7 To access files uploaded into the DSH, see below *Access to the DSH from your own desktop PC*.

4.4 Access to the DSH from your own desktop PC

To begin accessing any project data that has been uploaded into the DSH, users will need to use the Secure Desktop Access service. This service requires users to use the University's 2-factor authentication service (Duo) to verify their identity before they can gain access to any files in the DSH.

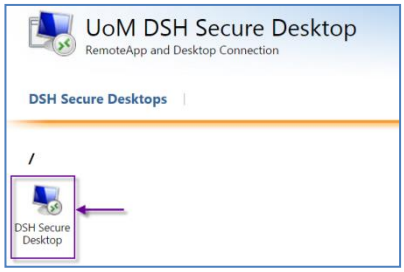
Please follow the instructions below to download the Remote Desktop Session icon onto your computer desktop. You will not be required to complete this activity when the icon has been added onto your computer desktop.

Step1) Download the Remote Desktop Session Icon

4.4.1 Go to https://desktop.dsh.manchester.ac.uk.

4.4.2 Enter your **usual University login details** into the login screen.

4.4.3 From the *UoM DSH Secure Desktop* screen, click the **DSH Secure Desktop icon**.



Note: only click the icon once to avoid initiating multiple remote desktop sessions.

4.4.4 The 'Save As' screen will appear. Select **desktop** from the option under the heading **Favourites** and click **Save**

4.4.5 The Remote Desktop Connection icon will appear on your desktop and can be used to access the DSH:

cpub-DSH_Secure_Deskt-DSH_Secure_Deskt-CmsRdsh.rdp

Step 2 Accessing your data using the Secure Access Service

Please ensure you have followed the steps detailed above if you do not have the Remote Desktop icon saved to your desktop.

4.4.6 Double click the Remote Desktop Connection icon and click **connect**

4.4.7 The Windows Security will appear. Enter your University password in the password box.

4.4.8 The DSH connection will now be established. Please note this may take a few seconds to initialise.

4.4.9 Once the connection has been established, you will be prompted to complete Two-Factor Authentication (2FA). Follow the instructions on the screen and on your device you registered with the 2FA service.

4.4.10 When you have successfully logged into your Secure Desktop session, open the **Windows Explorer file manager** to access your DSH data. The data you have access to will be found in two locations:

a. To access data that you have uploaded into the DSH platform (see Using the Secure Transfer Service), select the **Home (H:) drive** and then click the **Secure Transfer folder** to access your DSH files.
b. To access data that has been shared with you, select the **Project Data (I:) drive**. The project files you have access to will be listed.

If you do not have access to project files that you think you should have access to, contact your PI to review the access permissions.

4.5 Who can Access Data within DSH

Access to the Data Safe Haven is restricted to on-campus connectivity only. There is no provision via VPN to use the Data Safe Haven off-campus. Only the PI and Study IG Lead are authorised to **move data in or out** of the DSH. The project SLSP will specify the movement of the data into and out of the DSH.

The PI must approve with the RGEIT all other users and record this information in the study IG master file. Such users can only process the data within the DSH and this must match up with the SLSP developed for the study group. RGEIT will confirm with Research IT those users who can be granted access and will monitor this on a quarterly basis. Access rights will be granted by Research IT for each user to access specific project data via information received on the DSH landesk form, or from additional requests via the DSH amendments landesk form [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=c1d089d4-3449-4b92-9224-f1aa31c7762d].

The PI or IG Study Lead must notify the RGEIT of requests for new users. Research IT will not grant access to new users unless confirmation has been received from the RGEIT that checks

that the individual is listed in the data sharing agreement or SLSP and has completed the mandatory IG training as detailed in UM/17/SOP/NHSIGTK002 – Confidentiality Audit Procedure.

External collaborators who need access to the DSH will need UoM login credentials. This process must be initiated by the PI via the DSH amendments landesk form [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=c1d089d4-3449-4b92-9224-f1aa31c7762d]. External collaborators must have approval in place as demonstrated in the Data Sharing Agreement with the data provider and UoM and as subject to the same criteria as UoM staff in usage of the DSH. This will need to be recorded in the SLSP. To access the DSH the collaborator, once granted access by Research IT, will follow the same process as for other project users by following the instructions in 4.4 of this SOP.

4.6 Data Destruction from the laptop

Once you have transferred the data into the DSH, you should double check that that the transfer was successful by logging into the DSH from the laptop and checking the file in your project directory against that on the local laptop.

You will then immediately remove the local copy of the data from the hard drive of the laptopusing Blancco, by the PI or study IG Lead.

To remove the data please do the following on the laptop

1. Select 'Blancco File Eraser' icon from the Desktop
2. Using the '+' icon add all data that needs to be removed.
3. Select 'HMG Infosec, Higher Standard' as the Erasure Algortihm
4. Select 'Erase' to erase data securely.
5. A prompt asking 'Do you want erase all previous versions?' check 'Always leave previous versions' and select 'Leave previous versions' (please note system protection on the DSH laptop has been disabled, therefore no previous versions have been created).
6. A 'Operation Succcessful' message will appear once removal has been completed. Select 'View Log' this will open a separate window with a report of the data destruction.
7. Save a copy of the report.This must be emailed to the RGEIT and a copy retained in your study master file.

4.7 Removing Data from the DSH

Please note that all data removal, including for printing and reporting purposes will be audited by the RGEIT.

In keeping with the study Data Sharing Agreement with the data provider, it should be made clear for each study at the outset what the data removal requirements are and how this will be managed. The SLSP must state who can remove the data, (restricted to the PI and Study IG Lead or external collaborators if this is explicitly stated in the Data Sharing Agreement and permitted by the Data Provider), the level of data to be removed; anonymised or person identifiable (as the study requires). This will include running reports, discussing findings and writing papers. The SLSP will detail such requirements so that it is auditable by the RGEIT. It is noted that data removal can be completed at the users' desktop of the PI or the Study IG Lead by following the instructions in 4.3 and using the secure transfer service, this will not require using the laptop in the RGEIT office. Please note there will be no printing provision direct from DSH.

For studies where data removal is not known in advance, and not covered by the original Data Sharing Agreement and SLSP, the PI or Study IG Lead must put in a request to Research IT using the DSH amendments landesk form, question 7 [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=c1d089d4-3449-4b92-9224-f1aa31c7762d]. Research IT will notify RGEIT of the request for

confirmation. This is to ensure that the data removal has been verified as to the level of data to be removed (anonymised, pseudonymised), and to check that the need for the data removal is in line with any DSA or SLSP. In this instance the DSA and SLSP will require updating before the data can be removed.

4.8 Final removal of Data from the DSH

The final removal of the data from the DSH will depend on the data provider, funder requirements and will be written into the SLSP.

4.9 Adding data into the DSH and combining data sets

Researchers who need to add further data into the DSH that has not been obtained from the 3rd party data provider, or combine an existing data set with the data from the 3rd party data provider should do so within the DSH by adding in the less risky data to the data that is already housed in the DSH.

This process should have already been set out in the study SLSP before any data is entered into the DSH. Only the PI or Study IG Lead can add further data into the DSH. All additional data that does not meet the requirements for the DSH as noted in section 1 of this SOP, can be added to the DSH project folder from the desktop PC of the PI or Study IG Lead using the process in section 4.3 of this SOP.

For studies where data addition is not known in advance, and not covered by the original Data Sharing Agreement and SLSP, the PI or Study IG Lead must put in a request to Research IT using the DSH landesk amendments form, question 8 [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=c1d089d4-3449-4b92-9224-f1aa31c7762d]. Research IT will notify RGEIT of the request for confirmation.

4.10 Audit of data access and removal

The RGEIT will carry out regular audits of data access and removal to provide assurance to data providers that their data will remain within the DSH and not be removed without prior permission as stated in the SLSP and Data Sharing Agreement. The PI or Study IG Lead and all users will be advised that their access and activity within the DSH will be reviewed by the RGEIT. An audit of data removal and user access will involve checking DSH audit reports which detail when and what data has been removed against an agreed protocol for that study as detailed in the study SLSP as well as the location the user accesses the DSH (remote or via UoM desktop PC).

4.11 Additional requests for Software installation, or quota increases.

If a project requires further changes such as for software installation or quota increases, please submit these to Research IT using the DSH landesk amendments form [https://supportcentre.manchester.ac.uk/ServiceDesk.WebAccess/ss/object/open.rails?class_name=AssetManagement.Service&key=c1d089d4-3449-4b92-9224-f1aa31c7762d], question 9.

5 Consultation, Approval and Ratification Processes

5.1 Consultation and Communication with Stakeholders

All University NHS Digital data documents are written by a member of staff with relevant expertise and experience. Additional advice is sought from members of Research IT and the Information Governance Office within the University or external advisors, as necessary.

5.2 Document Approval Process

5.2.1 Standard Operating Procedures are approved by the Head of RGEIT and/or Associate Vice President for Compliance, Risk and Research Integrity.

5.5.2 Policies are ratified by the Research Compliance Committee.

6 Dissemination and Implementation

6.1 Dissemination

6.1.1 When approved, this document will be posted on the NHS Digital data pages of the University's Directorate of Business Engagement and Support Services website. Only the current version will be available.

6.1.2 All PIs/IG Leads will be notified by email when the latest version of the document is available.

6.2 Implementation of Procedural Documents

6.2.1 Training covering the contents of this document is delivered by the RGEIT.

6.2.2 Support and advice on the implementation of this document can be obtained via the Research Governance Officer (RGO) with responsibilities for NHS Digital data within the RGEIT.

7 Review, Monitoring Compliance with and the Effectiveness of Procedural Documents

7.1 Process for Monitoring Compliance and Effectiveness

7.1.1 The RGO will monitor compliance through regular audits of NHS Digital data master files.

7.1.2 Document contents will be reviewed against any changes to the applicable guidelines and regulations and taking into account any feedback received from Researchers or IG Leads.

7.1.3 The outcome of the review - and any resulting amendments – will be reported to the Research Compliance Committee.

7.2 Standards and Key Performance Indicators 'KPIs'

7.2.1 This document will be available on the University intranet.

7.2.2 This document must be reviewed at least every two years or when there are significant changes.

7.2.3 Awareness of the document will be delivered at University IG NHS Digital training sessions delivered by the RGEIT.

8 References and Bibliography

9 Associated University Documents

UM/17/SOP/NHSIGTK001:- Risk Assessment
UM/17/SOP/NHSIGTK002:- Confidentiality Audit Procedure
UM/17/SOP/NHSIGTK003:- Training Needs Analysis
UM/17/SOP/NHSIGTK004:- The Data Safe Haven
UM/17/SOP/NHSIGTK005:- IG Master File
UM/17/SOP/NHSIGTK006:- Data Sharing Agreements
UM/17/SOP/NHSIGTK007:- Destruction & Disposal of Sensitive Data on Isilon Procedure