



UoA STANDARD OPERATING PROCEDURE: NHS England data access, storage and management

Details:

| | |
|------------------------|--|
| Version number: | 4 |
| Authors | Suzanne Breeman (<i>NHSE researcher</i>), Mark Forrest (<i>NHS Gateway manager</i>), Martin Fraser (<i>Data centre manager</i>), Fiona Stuart (<i>Data Protection Officer</i>), Dean Phillips (<i>DDIS</i>), Juliette Snow (<i>R&I</i>), Brian Taylor (<i>NHS Gateway manager, Deputy</i>), Samantha Wileman (<i>HSRU QA manager</i>) |
| Issue date: | Oct 4, 2023 |
| Review date: | One year from issue date. |

Approval:

| | | |
|---|--|-------------------------|
| Approved by: | | |
| Professor Siladitya Bhattacharya |  <small>Siladitya bhattacharya (Oct 4, 2023 12:02 GMT+1)</small> | Oct 4, 2023 |
| Head of School of Medicine, Medical Sciences and Nutrition | Signature | Date |
| Tracey Slaven |  | |
| Information Governance Committee – Convener | Signature | Date Oct 4, 2023 |

Storage:

| | |
|------------------------------|---|
| Location of document: | |
| Electronic: | Q-Pulse |
| | https://www.abdn.ac.uk/clinicalresearchgovernance/sops/index.php |

Version history:

| Version | Description of Changes | Author <i>(role or dept.)</i> | Approved by | Approval date |
|---------|---|---|--|---------------|
| 1 | Document created to support the introduction of a new process for the management of NHS Digital (NHSD) data sets and derived data | Professor Phil Hannaford Mark Forrest Katie Wilde Martin Fraser Gail Smillie Mark Marrooth Gerry Paterson Alastair Matthews Derek Dawson | Professor P Hannaford (CLSM) | 09/05/17 |
| 2 | Update to document to enable the move of data to new storage infrastructure, remove reference to storage infrastructure (SRDS) and Colleges as both no longer exist. | Katie Wilde Mark Forrest Martin Fraser Dean Phillips | Professor Karl Leydecker (Principal's Office) | 25/02/21 |
| 3 | Major review and update of the document. Changes made to the 'Document management'. Background section includes more detailed information about NHSD Agreement and NHSD Data. Under Section 8, more detailed guidance and clarity given to staffs' responsibilities, and a new sub-section for 'Additional Researchers; and 'R&I' added. Under section 9, a new 'Data Breach' section has been added. | Suzanne Breeman <i>(NHSD researcher)</i> Mark Forrest <i>(NHSD Gateway manager)</i> Martin Fraser <i>(Data centre manager)</i> Iain Gray <i>(Data Protection Officer)</i> Dean Phillips <i>(DDIS)</i> Juliette Snow <i>(R&I)</i> Brian Taylor <i>(NHSD Gateway manager, Deputy)</i> Samantha Wileman <i>(HSRU QA manager)</i> | Professor S Bhattacharya (Head of School) Information Governance Committee Chair | 06/06/22 |
| 4 | The main update is change from NHSDigital (NHSD) to NHSEngland (NHSE); following the merger 1 February 2023. Also, updated format of SOP and minor updates to sections 8.6.6, 8.7.2, 9.2, 9.6.1 and 9.7.1. | Suzanne Breeman <i>(NHSE researcher)</i> Mark Forrest <i>(NHS Gateway manager)</i> Martin Fraser <i>(Data centre manager)</i> Fiona Stuart <i>(Data Protection Officer)</i> Dean Phillips <i>(DDIS)</i> Juliette Snow <i>(R&I)</i> Brian Taylor <i>(NHS Gateway manager, Deputy)</i> Samantha Wileman <i>(HSRU QA manager)</i> | Professor S Bhattacharya (Head of School) Information Governance Committee Convener | Oct 4, 2023 |

Contents

| | | |
|----|--------------------------------------|----|
| 1. | PURPOSE/INTRODUCTION | 4 |
| 2. | BACKGROUND | 4 |
| 3. | SCOPE | 5 |
| 4. | ASSOCIATED DOCUMENTS | 5 |
| 5. | REFERENCES | 5 |
| 6. | ABBREVIATIONS, TERMS AND DEFINITIONS | 5 |
| 7. | ROLES | 6 |
| 8. | RESPONSIBILITIES | 7 |
| 9. | PROCEDURES | 10 |

This Standard Operating Procedure (SOP) will be reviewed at least annually, or earlier should substantive changes to the UoA NHS England (NHSE) Data Sharing Framework Contract (DSFC), or any other agreements between NHS England and UoA (together referred to as NHSE Agreements), necessitate a review.

NOTE:

All printed copies of this SOP are UNCONTROLLED. Please ensure you are working on the most up-to-date version of this document. Revisions must include consultation with all the following sections: DDIS, R&I, CHaRT

1. Purpose / Introduction

To provide information and instruction to staff on the control of access, secure storage and management of NHSE data to ensure compliance with the current version of the UoA NHS England Data Sharing Framework Contract (CON-313306-V2W6S-DSFC-University of Aberdeen). **Adherence to this SOP is mandatory and will be subject to audit.** Any queries on this procedure should be directed to the NHS Gateway Manager at nhsgateway@abdn.ac.uk.

2. Background

The NHSE Agreements describe the requirements for the control of access, storage and management of NHSE Data (defined below) to ensure NHSE Data is kept secure, is managed in accordance with legal requirements including the Data Protection Act 2018 and UK GDPR, and that the technical environment is adequate for this purpose.

The NHSE Agreements include the following definitions in relation to the data UoA may receive under these agreements:

Data: the health or social care data specified that is provided by NHS England to UoA under a Data Sharing Agreement. This definition includes Data that is combined (wholly or in part) with other data or information; or aggregate (wholly or in part) with other data or information; or adapted (wholly or in part).

Derived Data: any NHSE Data (wholly or in part) that is manipulated to such a degree that it: (a) cannot be identified as originating or deriving from the NHSE 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 NHSE Data; and (c) has not at any time been verified by NHS England as not fulfilling the criteria (a) and (b) above.

For the purpose of this SOP, the term 'NHSE Data' and 'NHS Derived Data' shall be used to refer to the NHSE Agreements definition of Data and Derived Data, as described above.

The NHSE DSA includes the right of NHSE to request immediate and permanent destruction or deletion of NHSE Data and UoA is contractually obliged to respond promptly and appropriately to any such request.

NHSE Data remains owned by NHSE and needs to be held at a location where access to the NHSE Data can be appropriately controlled and deletion of NHSE Data can take place on request. Derived Data is owned by the UoA or a UoA collaborator and is subject to UoA research governance policies and procedures, as applicable.

NHSE advises that, where a researcher has ANY doubt about which category their data falls into, they should discuss this directly with NHSE and request written confirmation of the discussion and any outcome.

3. Scope

This SOP is limited to the control of access, storage and management of NHSE Data within the UoA and connected devices. It does not replace other policies or SOPs governing the management and use of such NHSE Data or Derived Data. Please see the UoA Research Governance Handbook for all other relevant information.

4. Associated documents

UoA NHS England Data Sharing Framework Contract (CON-313306-V2W6S-DSFC-University of Aberdeen)

Please contact R&I for a copy of the current version

UoA Research Governance Handbook: <https://www.abdn.ac.uk/staffnet/research/research-governance-10644.php#panel6326>

5. References

NHS England Site: <https://www.england.nhs.uk/about/protecting-and-safely-using-data-in-the-new-nhs-england>

6. Abbreviations, terms and definitions

| Abbreviation/Term | Definition |
|----------------------------|---|
| Additional Researcher | Named in the Information Asset Register, in addition to the Information Asset Owner and Named Researcher, and linked to a study specific NHSE dataset |
| CHaRT | Centre for Healthcare Randomised Trials |
| DDIS | Directorate of Digital and Information Services |
| DPO | Data Protection Officer |
| DSA | Data Sharing Agreement |
| DSFC | Data Sharing Framework Contract |
| IG | Information Governance |
| Information Asset Owner | A senior member of staff who is the nominated owner for one or more identified information assets within the UoA. In most cases it will be the UoA Principal Investigator (PI), but it may be delegated to another member of staff. |
| Information Asset Register | A list of personal and non-personal information assets held by the UoA |
| NHSE | NHS England |
| Named Researcher | Information Asset Owner or delegate (e.g. Trial Manager or Research Fellow) |
| R&I | Research and Innovation |
| Recipient | The Organisation detailed in the DSA (e.g. The University of Aberdeen) |
| SOP | Standard Operating Procedure |
| UoA | University of Aberdeen |
| VPN | Virtual Private Network |

7. Roles

| Role | Current Post Holder | Contact Details |
|-----------------------------------|----------------------------------|--|
| Named Researcher | Project dependant | Project dependant |
| Head of Research Institute | Project dependant | Project dependant |
| Head of School | Professor Siladitya Bhattacharya | s.bhattacharya@abdn.ac.uk |
| NHS Gateway Manager | Mark Forrest | nhsgateway@abdn.ac.uk |
| Deputy NHS Gateway Manager | Brian Taylor | nhsgateway@abdn.ac.uk |
| Data Centre Manager (DDIS) | Martin Fraser | martin.fraser@abdn.ac.uk |
| DDIS | Contact via Service Desk Call | servicedesk@abdn.ac.uk |
| Director of Research & Innovation | Dr Liz Rattray | e.rattray@abdn.ac.uk |

8. Responsibilities

8.1. The NAMED RESEARCHER is responsible for

- 8.1.1 Checking whether a DPIA has been completed for the study or documenting rationale for a DPIA not being required.
- 8.1.2 Ensuring that they are familiar with the requirements of the UoA NHS England Data Sharing Framework Contract (DSFC) and the project specific Data Sharing Agreement (DSA).
- 8.1.3 Undertaking appropriate annual Information Governance (IG) and Information Security (IS) training.
- 8.1.4 Advising the NHS Gateway Manager or deputy that they are to receive NHSE Data.
- 8.1.5 Provide NHS Gateway Manager with a copy of the authorised DSA for the requested NHSE Data.
- 8.1.6 Requesting a project specific folder from the Gateway Manager.
- 8.1.7 Ensuring that the **ONLY** device to be used to access the data prior to receipt of NHSE Data is a UoA managed device. Advise the NHS Gateway Manager which UoA device they will be using to access the NHSE Data.
- 8.1.8 Ensuring that all NHSE Data is stored in the UoA dedicated folder (as requested under 8.1.6).
- 8.1.9 Ensuring that the NHSE Data must not be replicated, copied or moved elsewhere. **The Named researcher, and Additional Researcher(s) as required, should therefore note that this is, and should remain, the only copy of the NHSE Data held at UoA.**
- 8.1.10 Ensuring that **NO** NHSE Data is downloaded to their personal device.
- 8.1.11 Considering what the requirements would be if an Additional Researcher needed access to the NHSE Data e.g., contract, training, contacting the Gateway Manger, reading this SOP and ensure these are enacted.
- 8.1.12 Ensuring Derived Data is held in a project specific shared drive.
- 8.1.13 Contacting R&I if Additional Researchers EXTERNAL to the UoA will need to access the NHSE Data to ensure that contractual arrangements are in place.
- 8.1.14 Contacting the NHS Gateway Manager when they no longer require access to the NHSE Data.
- 8.1.15 Contacting the NHS Gateway Manager when the Named Researcher no longer requires access to the NHSE Data.

8.2. Additional Researcher(s) of the data, are responsible for

- 8.2.1. Ensuring that they are familiar with the requirements of the UoA NHS England DSFC and the project specific DSA.
- 8.2.2. Undertaking appropriate annual IG and IS training.
- 8.2.3. Ensuring that the **ONLY** device to be used to access the data prior to receipt of NHSE Data is a UoA managed device. Advise the NHS Gateway Manager which UoA device they will be using to access the NHSE Data.
- 8.2.4. Ensuring that **NO** NHSE Data is downloaded to any personal device.

8.3. In the absence of the Named Researcher, the Head of Research Institute is responsible for:

- 8.3.1. Assuming NAMED RESEARCHER responsibilities for the NHSE Data and Derived Data, or re-assigning NHSE Data and Derived Data ownership.

8.4. In the absence of a Head of Research Institute, the Head of School is responsible for:

- 8.4.1. Assuming NAMED RESEARCHER responsibilities for the NHSE Data and Derived Data, or re-assigning NHSE Data and Derived Data ownership

8.5. The NHS Gateway Manager is responsible for:

- 8.5.1. Informing DDIS, following a request from the Named Researcher, that a new DSA has been authorised by NHSE and UoA. This is managed via the IT Service Desk (servicedesk@abdn.ac.uk).
- 8.5.2. Informing DDIS which UoA managed device will be used to access the NHSE Data.
- 8.5.3. Setting up a project specific folder with appropriate permissions following a request from the Named Researcher.
- 8.5.4. For confirming evidence of relevant annual IG training from the named researcher.
- 8.5.5. Removing or suspending access to approved researchers who have not undertaken annual training.
- 8.5.6. Receiving sensitive NHSE Data and storing it in the project specific folder.
- 8.5.7. Ensuring that all NHSE Data downloaded to the device is immediately deleted after transfer to the project specific folder.
- 8.5.8. Ensuring that any further requests for access conform to NHSE requirements and Additional Researchers have the necessary approvals and training in place before being given access to the NHSE Data.
- 8.5.9. On request of the Named Researcher, approving and implementing any subsequent changes to permissions.
- 8.5.10. On request of the Named Researcher, requesting retrieval of back-up Data from DDIS if required.
- 8.5.11. On request of the Named Researcher or NHSE, deleting NHSE Data and requesting, via the IT Service Desk (servicedesk@abdn.ac.uk) that DDIS deletes all corresponding back-ups of the NHSE Data. Data Centre Manager (DDIS) to be copied into the request.
- 8.5.12. Updating the Information Asset Register with received /deleted files, and ensuring it is reviewed annually.
- 8.5.13. Advising the Head of School, Head of Institute and Director of Research & Innovation of any requests from NHSE to delete NHSE Data

8.6. DDIS are responsible for:

- 8.6.1. On request from the NHS Gateway Manager, setting up permissions for the project specific folder.
- 8.6.2. Ensuring backup and recovery of NHSE Data.
- 8.6.3. On request from the NHS Gateway Manager, deleting all backup copies for the named file or folder.
- 8.6.4. Advising NHS Gateway Manager that deletion of the NHSE Data has been completed.
- 8.6.5. Ensuring any IT related changes that may have an impact on the DSA or DSFC (e.g. change of storage location etc) are communicated to the NHS Gateway Manager.
- 8.6.6. Ensuring whilst in the dedicated folder at rest, the NHSE Data is held in an encrypted state.

8.7. R&I are responsible for:

- 8.7.1 Following the current version of the *Research and Innovation Working Procedure for Managing NHS England Agreements* to ensure all NHSE Agreements are reviewed by the appropriate internal UoA stakeholders prior to signature by a UoA authorised signatory.
- 8.7.2 Ensuring the appropriate internal UoA stakeholders including the Named Researcher / Information Asset Owner, DDIS, Data Protection Officer (DPO) and Gateway Manager receive copies of signed NHSE Agreements.

9. Procedures

9.1. Receiving data

- 9.1.1. The Named Researcher is responsible for applying to access NHSE Data through the NHSE DARS Portal. Once the request has been approved by NHSE a Data Sharing Agreement will be issued to the UoA authorised signatory through the DARS portal.
- 9.1.2. In accordance with the current version of the *Research and Innovation Working Procedure for Managing NHS England Agreements*, Research and Innovation will ensure appropriate due diligence of the NHSE Agreement is completed before arranging signature by an authorised signatory and circulation of the fully signed NHSE Agreement to all internal stakeholders.
- 9.1.3. The NHS Gateway Manager **MUST** advise the DDIS Service Desk that the Named Researcher plans to access NHSE Data via their UoA managed device.
- 9.1.4. The NHS Gateway Manager will download the NHSE Data from the link provided by NHSE; only downloading to the UoA managed device.
- 9.1.5. The NHS Gateway Manager will then move this file in to the agreed file share managed by the Gateway Manager.
- 9.1.6. The Named Researcher will notify the NHS Gateway Manager with the end date for data retention so the UoA Information Asset Register can then be updated.
- 9.1.7. The Named Researcher will access the NHSE Data in the new location to ensure successful transfer.
- 9.1.8. The NHS Gateway Manager will then delete the copy of the NHSE Data that is on the UoA managed device (In the Downloads file)
- 9.1.9. The NHS Gateway Manager will then empty their Recycle Bin (Right click on Recycle Bin and Click Empty)

9.2 Storage and processing

All source NHSE Data is stored in the UoA Data Centre 1 and 2.

- 9.2.1 The Named Researcher will open the file in the agreed file share and check the Data.
- 9.2.2 The Named Researcher will only store NHSE Data retrieved from NHSE in the allocated project specific folder.

9.2 Access

- 9.3.1 The NHS Gateway Manager will manage and update all permissions to the NHSE Data. The Named Researcher will advise the NHS Gateway Manager if any Additional Researchers require access to the NHSE Data (read or read/write against each Additional Researcher).
- 9.3.2 The Named Researcher, and Additional Researcher(s) if relevant, will only access the NHSE Data from UoA managed devices. There will be no access to the NHSE Data from non-corporate or personal devices e.g. via the VPN (Virtual Private Network).

9.4 Backup

- 9.4.1 DDIS will back-up all NHSE Data held to two sets of NHSE specific backup tapes, ensuring the Data is easily identifiable, and easily deleted on request.
- 9.4.2 DDIS will store each set of back-up tapes in a locked, restricted access room, in separate UoA buildings, with access controlled by DDIS.

9.5 Retrieval of NHSE Data from backups

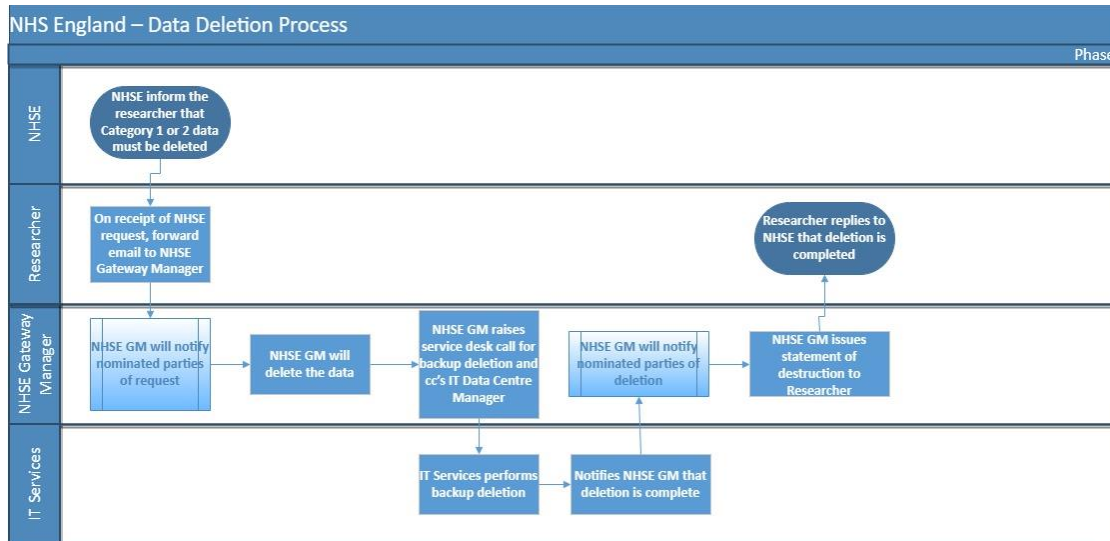
- 9.5.1 If the Named Researcher requires retrieval of NHSE Data from back-ups, this request will be made through the NHS Gateway Manager.
- 9.5.2 The NHS Gateway Manager will request retrieval of the data from DDIS via the IT Service Desk, also advising of the file path where the NHSE Data should be restored to.
- 9.5.3 DDIS will retrieve the last version of the NHSE Data (unless other specified) from back-up and restore to nominated location.
- 9.5.4 The NHS Gateway Manager will advise the Named Researcher that the NHSE Data is now restored and available.

9.6 Data Deletion

- 9.6.1 Following a request from NHSE for deletion of the NHSE Data the Named Researcher must immediately forward the written request to NHS Gateway Manager.
- 9.6.2 The NHS Gateway Manager will then inform the following of this request:
- Director of Research & Innovation (or local representative)
 - Head of School
 - Head of Research Institute
- 9.6.3 The NHS Gateway Manager will delete the NHSE Data from the dedicated folder.
- 9.6.4 The NHS Gateway Manager will then formally request deletion of all corresponding back-up NHSE Data via an IT Service Desk call, copied to the IT Data Centre Manager. This request needs to include the full path(s) of all file(s) that need to be deleted.
- 9.6.5 DDIS will complete the deletion and advise the NHS Gateway Manager via the Service Desk support system that it has been done.
- 9.6.6 The NHS Gateway Manager will advise the below parties when this has been completed:
- Director of Research & Innovation (or local representative)
 - Head of School
 - Head of Research Institute
- 9.6.7 NHS Gateway Manager will issue a statement of destruction to the Named Researcher.
- 9.6.8 NHS Gateway Manager will log the NHSE Data as having been deleted in the Information Asset Register.
- 9.6.9 The Named Researcher is responsible for then advising NHSE that the deletion request has been completed.

Data Deletion Process Workflow

This flow diagram details the NHSE technical requirements and the UoA response



9.7 Data Breach

A Personal Data Breach of NHSE data means a breach of data security or information security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, NHSE personal data in terms of the DSFC. This includes breaches that are the result of both accidental and deliberate causes.

- 9.7.1 In the event of a NHSE Data Breach, or a possible Data Breach, the Information Asset Owner, Named Research and/or Additional Researcher must notify the UoA's Data Protection Officer as soon as possible (within 48 hrs).
- 9.7.2 The Information Asset Owner, Named Research and/or Additional researcher must provide the DPO with enough information to allow them to assess the incident. Please refer to <https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8626> for full information of recording and reporting.
- 9.7.3 The UoA Data Protection Officer (DPO), as the appropriate delegate for the Recipient, must then notify NHSE of any Data Breach as soon as possible.
- 9.7.4 The DPO must refer to Section 4.1.8 of the DSA to understand the Recipient's contractual responsibilities regarding the reporting of the data breach. They will be required to either complete a 'Serious Incident requiring Investigation' report or they will need to assess whether to notify the Information Commissioner's office (ICO) of the Data Breach.
- 9.7.5 In addition, if the Recipient receives any communication from the (ICO) which relates to such Personal Data, they must report this to NHSE immediately, unless explicitly prohibited from doing so by the ICO.











NHS England Data Management SOP V4

Final Audit Report

2023-10-04

| | |
|-----------------|--|
| Created: | 2023-10-03 |
| By: | Juliette Snow (j.e.snow@abdn.ac.uk) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAIL0X6f2aOWL8CLNYDDwl-fmQU9DOK-DZ |

"NHS England Data Management SOP V4" History

-  Document created by Juliette Snow (j.e.snow@abdn.ac.uk)
2023-10-03 - 15:25:56 GMT- IP address: 139.133.179.30
-  Document emailed to s.bhattacharya@abdn.ac.uk for signature
2023-10-03 - 15:43:12 GMT
-  Email viewed by s.bhattacharya@abdn.ac.uk
2023-10-03 - 15:51:14 GMT- IP address: 140.248.40.25
-  Signer s.bhattacharya@abdn.ac.uk entered name at signing as Siladitya bhattacharya
2023-10-04 - 11:02:21 GMT- IP address: 139.133.192.22
-  Document e-signed by Siladitya bhattacharya (s.bhattacharya@abdn.ac.uk)
Signature Date: 2023-10-04 - 11:02:23 GMT - Time Source: server- IP address: 139.133.192.22
-  Document emailed to tracey.slaven@abdn.ac.uk for signature
2023-10-04 - 11:02:25 GMT
-  Email viewed by tracey.slaven@abdn.ac.uk
2023-10-04 - 12:47:37 GMT- IP address: 139.133.212.158
-  Signer tracey.slaven@abdn.ac.uk entered name at signing as Tracey Slaven
2023-10-04 - 12:48:03 GMT- IP address: 139.133.212.158
-  Document e-signed by Tracey Slaven (tracey.slaven@abdn.ac.uk)
Signature Date: 2023-10-04 - 12:48:05 GMT - Time Source: server- IP address: 139.133.212.158
-  Agreement completed.
2023-10-04 - 12:48:05 GMT