HIC SERVICES STANDARD OPERATING PROCEDURE

Data Security

SOP NUMBER: HIC Services SOP 01
VERSION NUMBER: 10.0
EFFECTIVE DATE: 15/01/2021
DOCUMENT SECURITY LEVEL: Open
REVIEW DATE: This SOP will be reviewed at least every 12 months, or at other times as requested by: HIC Information Governance Committee
AUTHOR: Duncan Heather
DATE APPROVED BY THE INFORMATION GOVERNANCE COMMITTEE: 15/01/2021
DATE APPROVED BY THE HIC EXEC COMMITTEE: 10/11/2020
DATE REVIEWED BY HIC OPERATIONS GROUP: N/A
CONTACT PERSON FOR THIS SOP: Duncan Heather, HIC Governance Manager, d.heather@dundee.ac.uk
**DOCUMENT REVIEW AND REVISION HISTORY:**

<table>
<thead>
<tr>
<th>Version Number:</th>
<th>Edited by (job title):</th>
<th>Effective Date:</th>
<th>Details of editions made:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/09/13</td>
<td>This is a new SOP which expands on a subset of policies and supersedes Version 6 of the HIC Standard Operating Procedure, Management of HIC Datasets. Effective from 1st August 2011.</td>
</tr>
<tr>
<td>1.1</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>15/05/14</td>
<td>Edit governance diagram to add “HIC Governance Committee”</td>
</tr>
<tr>
<td>2.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/08/14</td>
<td>Add new section: Access to HIC secure rooms, NHS network and data</td>
</tr>
<tr>
<td>3.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/01/15</td>
<td>General review and update</td>
</tr>
<tr>
<td>4.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/08/15</td>
<td>Added sections for Teleworking, Clear screens and desks and Personal &amp; Portable devices</td>
</tr>
<tr>
<td>5.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/01/16</td>
<td>Extended types of secure data transfer methods permitted and added more detail about Safe Haven restrictions for users. Revised safe haven diagram at 5.8 to reflect move away from Citrix</td>
</tr>
<tr>
<td>6.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/04/16</td>
<td>Add details re: restricting release of free text (5.7.1.4), anonymisation of image files (5.7.1.9), transferring image files (5.9.1.4 &amp; 5.9.1.5) and updating name of Governance Committee to Information Governance Committee</td>
</tr>
<tr>
<td>7.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/12/17</td>
<td>5.1.1.4 changed from UoD Policy to UoD best practice guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.1.1.6 updated to reflect ISO 27001 Certification requirement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.2.1.2 removed unnecessary verbiage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.2.2.2 updated to Non-Disclosure agreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.2.3.6 updated to reflect appropriate roles</td>
</tr>
<tr>
<td>8.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>08/11/18</td>
<td>Added section 5.8 reversing the anonymisation process- moved from HIC SOP 03 and 5.6.1.8 to reflect a backup process if PM system is down when releasing data</td>
</tr>
<tr>
<td>Section</td>
<td>Author</td>
<td>Date</td>
<td>Changes</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>9.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>17/03/2020</td>
<td>Updated staff access section 5.2. Added new 5.9.4 section about releasing individual-level derived data from Safe Haven for consented genetic studies. Amended section 5.3 Teleworking</td>
</tr>
<tr>
<td></td>
<td>Rachael Torano (Business Support)</td>
<td>14/05/2020</td>
<td>Updated with new and approved Header Changes made to cover page to include Op’s review date as agreed at the HIC Information Governance Meeting As agreed by the HIC Governance Committee signatures have been removed from cover page and Document Review and Revision History table has been updated to include review dates and notes</td>
</tr>
<tr>
<td>10.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>15/01/2021</td>
<td>Added to security check requirement for non-UK resident new HIC staff in 5.2.1.2</td>
</tr>
<tr>
<td></td>
<td>Jenn Johnson (HIC Business Support)</td>
<td>11/11/2021</td>
<td>Updated header and footer. This revision does not need to be approved by Committee’s as previously agreed and does not constitute a version change.</td>
</tr>
</tbody>
</table>

*Draft and Archived/Obsolete revisions are not to be used. Access current versioning system to verify revision.*
1. PURPOSE

Health Informatics Centre Services (HIC Services) is a University Research Support Unit operating within the Tayside Medical Science Centre (TASC) at the University of Dundee, in collaboration with NHS Tayside and NHS Fife. HIC Services provides Data Users with linked, anonymised information derived mostly from large Population Based Health Datasets, owned mainly by the NHS and the University of Dundee. HIC also develops data collection software, provides data entry and securely hosts data for research use.

This SOP describes HIC Services’ measures to provide security, confidentiality and privacy to data received, managed and supplied by HIC Services. The following areas are covered:

- An overview of HIC Services data security
- Access to HIC secure rooms, NHS network and data
- Receiving new data
- Providing a project dataset to data users
- Project Level Anonymisation
- The HIC Services Safe Haven

2. SCOPE

This SOP covers all of the projects and tasks which HIC undertake. It is applicable to all HIC staff. This SOP is will be made available to all users and potential users of the HIC Service and will be externally visible on the public HIC website.

3. DEFINITIONS

For overall Definitions see HIC Services SOP Appendix B – Definitions.

4. RESPONSIBILITIES

- **HIC Director** – Responsible for overall HIC security policy and implementation
- **Process Manager** – Ensuring SOPs are followed by team
- **Governance Manager** – Monitoring compliance, handling significant events, keeping SOP up to date
- **All HIC Staff** – Responsible for adherence to the SOP as specified
5. POLICY
For overall Policy see HIC Services SOP Appendix A – Policy.

5.1 Data Security Policy

5.1.1 Overview

HIC Services' highest priority is to address information governance, data security and confidentiality issues, whilst providing researchers with secure access to linked, anonymised information, recruitment mailing services, data entry and bespoke data collection software tools.
5.1.1.1 Identifiable data will be received by the HIC Data Analyst via secure, encrypted transmission and will be stored, quality assured and processed on secure servers, in secure work areas.

5.1.1.2 The physical premises have access-controls to the rooms containing HIC Technical Staff.
5.1.1.3 The access-controlled server rooms, accessible only to IT Administrators, contain 2 separate networks:
- NHS, which holds all identifiable NHS data
- University, which hosts the remote-access HIC Services Safe Haven and research data.

5.1.1.4 Strict login access controls are in place across all HIC networks, including the NHS network and Safe Haven, in line with University of Dundee password best practice guide.

5.1.1.5 Records of all projects, approvals and data releases are kept on the HIC Services Project Management System.

5.1.1.6 HIC Services facilities and processes are audited at least once annually by external auditors as part of HIC Services ISO27001 Certification.

5.1.1.7 HIC Services procedures are reviewed and approved by the HIC Information Governance Committee. The Committee receives a copy of the annual external audit and the actions HIC Services have taken in response to issues raised by the auditors.

5.2 Access to HIC Secure Rooms, HIC NHS and University IT networks and Data

5.2.1.1 New HIC Technical staff, as defined in HIC Services SOP Appendix B - Definitions, are added to the document HIC Services SOP Appendix C - Contacts and Roles.

5.2.1.2 New HIC Technical staff will not be given access to confidential HIC data or live HIC external production systems until their Disclosure Scotland security check has been completed and a certificate received. For new HIC Technical Staff not already resident in the UK, a local police record check will be required in place of a Disclosure Scotland check.

5.2.2 Access to Secure Rooms

5.2.2.1 HIC staff will have controlled access to secure rooms and the HIC IT networks, as required.

5.2.2.2 All HIC staff will read and sign a copy of the HIC Staff Confidentiality Agreement.

5.2.2.3 Other University staff and visitors will not be given access to the secure room unless they have signed-in and are accompanied by someone that has secure area access.

5.2.3 Access to HIC NHS and University network and Data

5.2.3.1 Access to specific datasets within the HIC NHS and University networks will be decided and actioned by the relevant HIC Services Process Manager or their designated deputy.

5.2.3.2 Data access will only be provided to HIC Technical Staff on request to specific named datasets.

5.2.3.3 HIC Technical Staff must request access to a named dataset via the Process Manager, or their designated deputy.

5.2.3.4 Each dataset access request must be endorsed by the HIC Technical Staff member’s supervisor.

5.2.3.5 When access is no longer required, the HIC Technical Staff member, or their supervisor, will request removal from the dataset’s access list.
5.2.3.6 Every 6 months, the network and dataset access lists will be audited to reconfirm the Technical Staff’s access.

5.2.4 Secure Room and Dataset Access Removal

5.2.4.1 When HIC Technical Staff no longer need access to the HIC IT network, or a specific named dataset, their supervisor is responsible for making a request to the HIC IT Administrator, copying in the Process Manager, to have their access rights removed.

5.2.4.2 When a HIC Technical Staff member leaves HIC all secure room, HIC IT network and dataset access will be removed. This will be triggered by relevant Process Manager, who will inform the HIC IT Administrator of the changed access requirement.

5.3 Teleworking

5.3.1.1 This allows an employee to work securely at home or an alternate location to their base. This can lead to a reduction in commuting, reduce workspace constraints, allow for working in a business continuity scenario, and enhance employee productivity and satisfaction.

5.3.1.2 HIC policy is to allow employees to telework when it has been determined that teleworking will allow work to be performed effectively, securely and productively, provided:

- Access is via approved University or NHS Tayside VPN access and data remains on those networks.
- Only University "Permission to Connect" authorised, encrypted devices are used, as defined in University of Dundee Network Connection Policy.

5.3.1.3 No hard copy data falling into the University classification of confidential (See University Information Classification Scheme) should be taken off site unless approved in advance. Guidance can be provided by the University Archive, Records Management and Museum Services (ARMMS).

5.4 Clear Screen and Clear Desk

5.4.1.1 To avoid inappropriate access to computing devices and to restrict unauthorised access to information on display screens:

- Users must log off or lock their computers when unattended
- A password protected screensaver should be set to activate after a maximum of 15 minutes of inactivity on all devices capable of such.

5.4.1.2 All information held in a physical format marked, or falling into the University category of confidential must be appropriately secured when staff are absent from their workplace and at the end of each working day, to reduce its potential exposure to unauthorised access.
5.5 Portable and Personal Devices

5.5.1.1 Laptops, tablets and other mobile devices connecting to the University or NHS network or holding University or holding potentially confidential organisational information must be protected by a password or pin code in line with the University’s password best practice guide.

5.5.1.2 When working in public areas such as restaurants, on trains or aircraft, care should be taken to prevent others from being able to view potentially sensitive information.

5.5.1.3 Any changes made to files (or data) normally stored on University shared network drives whilst not connected to the University’s Network should be copied back to the normal storage location at the next opportunity.

5.5.1.4 Any confidential data held on mobile devices must be encrypted.

5.5.1.5 In the event of loss or theft of a mobile device the user should contact the HIC Governance Manager who will follow SOP03 handling significant events.

5.5.1.6 Use of personal devices must be used in adherence with the University’s Acceptable use policy, including receiving University "Permission to Connect" and encryption before connecting to the University network.

5.6 Releasing a Project Dataset

5.6.1.1 Release of a Project Dataset is undertaken only by a HIC Data Analyst.

5.6.1.2 The Project Dataset will only be released to an Approved Data User by the HIC Data Analyst when all the requirements for such release are met.

5.6.1.3 The release only provides data for the cohort, aims and methods specified in the Project Description, which is stored on the PM System.

5.6.1.4 An Approved Data User must be linked to the project, identified on the PM System.

5.6.1.5 The Data Governance section of the PM System must have been completed by the HIC Governance Manager, confirming that all approvals are in place and stored on the PM System.

5.6.1.6 Details of all data releases will be recorded by the HIC Data Analyst on the PM system. The project Data Requirements and Data Release details of all data extracted and generated by the HIC Data Analyst, will be stored within the Project folder. Project level anonymisation will be carried out on the Project Dataset. This anonymisation ensures that each Project Dataset has a unique series of anonymised codes. This step is not required if the Approved Project has approvals to receive patient identifiable data.

5.6.1.7 All Approved Project Datasets will be released onto a secure, HIC Services-managed server within the HIC Services Safe Haven environment. Approved Data Users registered on the PM System will be provided a login to remotely access and carry out analyses on their dataset. Data will not be provided directly to Approved Data Users except where:
• Projects began prior to 1st November 2011 and already have data released directly and
the project is not yet complete.
• Project datasets are of consented participants and the project approvals do not require
use of the HIC Services Safe Haven.
• Data is being exported to other Safe Havens.

5.6.1.8 If the PM system is not available, any required governance checks will be recorded on
paper, and appended to PM system as soon as practicable, once access is restored.

5.7 Project-Level Anonymisation

5.7.1.1 Every project dataset will be uniquely anonymised before being made available to an
Approved Data User, unless identifiable data is required and is specifically approved by
the Data Controller.

5.7.1.2 The Pro-CHI is generated by the HIC Data Analyst to uniquely anonymise a typical NHS
dataset CHI number. This capability is located on a secure server, accessible only by the
HIC Data Analyst and the IT Administrator.

5.7.1.3 The anonymisation process removes all names and addresses from the dataset. As
standard it also:
• Uniquely anonymises the CHI into a project-specific pseudo-CHI (Pro-CHI)
• The date of birth – standard anonymisation is 3 months whereby the day will become
‘01’ and the month will become the middle of the appropriate quarter year e.g.
24/01/2005 will be anonymised as 01/02/2005).
• The postcode is restricted to postcode district / outward postcode only by removing
the last 3 digits, e.g. DD1, DD10.
• The GP code, the GMC number (General Medical Council registration number), the GP
Practice code and the Pharmacy code are all replaced by anonymous versions.
• If data is being provided via HIC Services that has already been effectively anonymised
elsewhere, this procedure may not need to be repeated by HIC Services.
• Where there is no CHI a unique pseudonymised identifier will be allocated to each
individual
• Aggregated data provided for study feasibility will not show values <5.

5.7.1.4 Free text fields, which may contain identifying information, are not provided as part of a
Project Dataset unless specific Caldicott Approval is obtained.

5.7.1.5 These steps will help ensure that identification of individual patients is not possible, while
retaining the ability to link patient data across multiple data sets for a particular project.

5.7.1.6 Any request to the HIC Data Analyst for more detail about any of the Anonymised Data
items listed above will be treated as a request for identifiable data, which will require
study-specific Caldicott Guardian approval.
5.7.1.7 The Pro-CHI is project-specific ensuring that data provided to any one project remains within the bounds of linkage as approved for that project.

5.7.1.8 The Pro-CHI allows traceability of any HIC Services Project Dataset to the source of the data and the subsequent Approved Data User for that data.

5.7.1.9 The metadata in DICOM (Digital Imaging and Communications in Medicine) image files is anonymised using DICOM software and any fields which may contain Identifiable data (e.g. free text) are removed before the Pro-CHI process is applied.
5.8 Reversing the Anonymisation Process

5.8.1 In addition to the reason stated in section 5.2, there are other occasions when it is necessary to reverse the anonymisation process and go back to the original source of the data. For example:

- Over the course of a study additional data is sometimes required to help achieve the outcomes of the study, potentially from a wider data source. Individuals would need to be identified to be able to request this additional data
- To validate findings, e.g. from information in the patient paper file
- To identify individuals who may, for their own benefit, be in need of further tests or treatment. This action would only be initiated by the opinion of a qualified clinician collaborating with the study

5.8.2 When reversal becomes necessary, permission must be sought from the Caldicott Guardian of the NHS Board of the patient’s residence.

5.8.3 This permission must specify which individuals can have access to any identifiable data (e.g. a patient’s GP, or the Approved Data User who will be viewing patient files).

5.8.4 Once this approval has been obtained, it will be logged onto the PM System.

5.8.5 Details of the request from the Approved Data User and release of any identifiable or additional anonymised data will also be added to the PM System.
5.9 The HIC Services Safe Haven

The infrastructure model is illustrated below:

5.9.1 Overview

5.9.1.1 The HIC Services Safe Haven utilises a secure remote-access environment. In this model data are no longer released externally to Approved Data Users for analysis on their own computers but placed on a HIC server, within a restricted, secure IT environment, where the Approved Data User is given secure remote access to analyse it. Access to the HIC Services Safe Haven by Approved Data Users is restricted and controlled by Active Directory access control lists and global security groups.

5.9.1.2 Commonly-used tools for data analysis are provided for use within this environment and approved Data Users can securely access this server from anywhere. The Approved Data User is restricted – i.e. cannot print, access the internet or export data. Approved Data Users are not permitted to copy individual-level data outside the safe haven via any means including, for example (not exhaustive); photographic, recording, screen grabbing and note taking.

5.9.1.3 User-specific files (e.g. look-up tables, stats scripts) can be imported to a user’s personal folder (i.e. not available to other HIC Services Safe Haven users) via the HIC IT
Administrator after review by the HIC Data Analyst. Users can make copies available to project collaborators via the shared project folder if required.

5.9.1.4 The HIC IT Administrator will provide details about current available software and versions on request.

5.9.2 Account Creation

5.9.2.1 All account creation requests must be initiated by a HIC Data Analyst. Accounts will only be granted to allow an Approved Data User to access their active Approved Project. All project approvals must be in place and all Approved Data Users will need to have read and signed the latest HIC Services Data User Declaration, before being given access to the Safe Haven. See flow diagram below.
5.9.3  **Output disclosure control – Unconsented NHS data studies**

5.9.3.1 To enable an output file to be removed the Approved Data User will move the file to the output directory within their HIC Services Safe Haven personal directory.

5.9.3.2 No individual-level data are permitted to be removed from the HIC Services Safe Haven. Only analysis outputs e.g. reports, summaries, aggregates, graphs etc. may be removed.

5.9.3.3 The output file(s) will be reviewed by a HIC Data Analyst or IT Administrator by no later than 11am the next working day and, once verified as not containing individual-level data, emailed to the Approved Data User.

5.9.4  **Output disclosure control – Consented Bio-resource data studies**

5.9.4.1 To enable an output file to be removed the Approved Data User will move the file to the output directory within their HIC Services Safe Haven personal directory.

5.9.4.2 Individual-level data are permitted to be removed from the HIC Services Safe Haven, but will be limited to containing data derived from the source data, e.g.:

- Study ID
- Sex (M/F)
- Age (not DOB)
- Diagnostic or event status (aggregated from multiple hospital entries and multiple ICD10 codes and other sources)
- Aggregated Biochemical values. (e.g. mean untreated Cholesterol)
- Drug response. (e.g. model derived beta or odds ratio; or absolute or percentage change in biochemical parameter)
- Drug adherence (% prescription encashment)
- Duration of treatment (time-not calendar period)

5.9.4.3 No dates will be included in the release of derived data.

5.9.4.4 The output file(s) will be reviewed by a HIC Data Analyst or IT Administrator by no later than 11am the next working day and, once verified as not containing dates, emailed to the Approved Data User.

5.9.5  **Importing and hosting Research Datasets from external sources**

5.9.5.1 Research data not supplied by HIC, may be hosted in the HIC Services Safe Haven for analysis by Approved Data Users. This will require an approval from the appropriate Data Controller for the data.

5.9.5.2 The Approved Data User can request the return of the data.
5.10 Transfer of Data To and From HIC

5.10.1 Only the HIC Data Analyst will manage/process these datasets.

5.10.1.1 Datasets will be transferred by the HIC Data Analyst either through an existing arrangement (e.g. Agreed procedure or Service Level Agreement), or with a new source (e.g. data collected by a researcher).

5.10.1.2 HIC Services will require written approval from dataset owners (e.g. Caldicott Guardian for NHS data) prior to releasing data from these datasets.

5.10.1.3 • Identifiable data will be received by the HIC Data Analyst via secure, password encrypted transmission or file. The file password will be communicated separately.

5.10.1.4 Datasets should not be transferred via portable media (e.g. CD/DVD or memory stick), except high-volume transfers (e.g. Image data – see next item) where electronic transfer may not be feasible, or unsecured non-NHS email. If HIC Services receives data on portable media or unsecured non-NHS email unexpectedly the data will be transferred to a secure server on the HIC IT network, and the portable media archived, if portable media used. The sender will be told not to use portable media or unsecured email for any subsequent transfers of data.

5.10.1.5 Imaging datasets and other high-volume datasets may be transferred on encrypted hard disk in cases where the network infrastructure is not capable of transferring the required volume of data, e.g. limited bandwidth availability where data cannot be transferred in an acceptable amount of time without disruption to NHS clinical and business network traffic.

5.10.1.6 Identifiable information will not be sent to HIC Services by fax, as HIC Services doesn’t have one.

5.10.1.7 On receipt of the dataset, the HIC Data Analyst will load the data onto secure servers. The servers reside on the HIC IT network and are only accessible to the HIC Data Analyst and the IT Administrator.

5.10.1.8 Data Entry staff have restricted access to add CHI numbers to datasets, as required, using the appropriate software program.
5.11 HIC Approved Methods of Transfer

5.11.1.1 All data transferred to and from HIC will utilise one of the following methods.

5.11.1.2 Secure transfer mechanism:
- Internal NHS email to NHS email.
- NHS Secure File Transfer system (NHS network only).
- Transfer via the HIC Secure Customer Portal (https).
- Secure File Transfer Protocol (SFTP).

5.11.1.3 Alternative transfer methods. In the event that the above mechanisms are not available other transfer mechanisms (such as email or FTP) may be considered. Any file must be secured using one of the following approved secure methods:
- Advanced Encryption Standard compression (e.g. AES-256 Zip).
- Asymmetric encryption (e.g. PGP Public Private Key cryptography).

5.11.1.4 Identifiable, unconsented NHS data will always be transferred within the NHS network only.

6. APPLICABLE REFERENCES

- HIC Services SOP 02 Data Access Approvals
- HIC Services SOP 03 Handling HIC Services Data Events
- HIC Services SOP 04 Archiving a Project Dataset
- HIC Services Staff Confidentiality Agreement
- HIC Services Data User Declaration
- HIC Services SOP Appendix A – Policy
- HIC Services SOP Appendix B - Definitions
- HIC Services SOP Appendix C – Roles and Contact Details
- University of Dundee Network Connection Policy
- University of Dundee Acceptable Use Policy