Hic services STANDARD OPERATING PROCEDURE

Data Entry Office Security

SOP NUMBER: HIC Services SOP 05
VERSION NUMBER: 4.0
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 EXECUTIVE 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

Copyright Health Informatics Centre. All rights reserved. May not be reproduced without permission. All hard copies should be checked against the current electronic version within current versioning system prior to use and destroyed promptly thereafter. All hard copies are considered Uncontrolled documents.
### 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>2.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>01/01/14</td>
<td>General review and update</td>
</tr>
<tr>
<td>2.1</td>
<td>Keith Milburn (ADP Manager)</td>
<td>01/05/18</td>
<td>Removal of section referring to an office key from old CIB offices. Removal of 5.1.6 and addition of 5.1.5.3 which makes it clear that out of hours working is no longer permitted.</td>
</tr>
<tr>
<td>3.0</td>
<td>Duncan Heather (HIC Governance Manager)</td>
<td>08/11/18</td>
<td>Revised staff confidentiality agreement references</td>
</tr>
</tbody>
</table>
4.0  Adrian Clatworthy (Business Support Co-Ordinator)  15/01/2021  Updated to reflect new Business Support Team structure

*Draft and Archived/Obsolete revisions are not to be used.*

*Access current versioning system to verify revision.*
1. PURPOSE
The HIC Business Support team carries out data entry within a secure office at Ninewells Hospital. In addition to wider HIC administrative support activities, it receives and processes incoming NHS data relating to the community-dispensed prescription dataset. The team also provides general clerical support to individual research projects, including project-specific data entry for the Tayside Clinical Trials Unit (TCTU) and handling the receipt and dispatch of paper data and mail.

The management of staff, resources and costs are the responsibility of the University of Dundee via the HIC Executive Committee. Day-to-day management responsibilities are carried out by the Team Manager and the Senior Business Support Administrators.

This SOP defines the procedures surrounding the maintenance of security at the HIC Business Support data entry office to protect the confidentiality of data processed within the premises. This includes:
- Electronic Data Security
- General Security
- Visitors to the office
- Staff Entry/Exit Procedures

2. SCOPE
This SOP covers all of the projects and data-related tasks which HIC undertake which involve the HIC Business Support Team. It is applicable to all the HIC Business Support staff involved with recruitment and data entry activities involving patient data and their managers. This SOP is 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 Entry Security Policy

5.1.1 Electronic Data Security

5.1.1.1 The Business Support Team processes non-consented NHS patient-identifiable electronic images and data. This is all processed within the secure NHS network and the NHS data and images required by HIC Business Support for data entry are held on secure NHS-network servers. The patient data viewed by HIC Business Support Staff while carrying out their work is strictly confidential.

5.1.1.2 The Business Support Team also processes consented study data, mainly on behalf of the Tayside Clinical Trials Unit (TCTU). These data are processed via secure login to web-based study-specific databases.

5.1.2 General Security

Adherence to these procedures is required by all who work in the team to ensure that, at all times, the HIC Business Support data entry office is secure:

5.1.2.1 Access to the office is restricted by a coded door entry system.

5.1.2.2 Data entry monitors must be fully screened from observation by visitors.

5.1.2.3 Any patient-identifiable paper-based data to be processed and returned to the respective owner must be logged both in and out. While it is kept it will be stored in a locked cabinet or a locked storeroom when not in active use.

5.1.2.4 New employees will read and sign the HIC Staff Confidentiality Agreement.

5.1.2.5 Staff use unique log-ins and passwords to access programs and data for processing. These are to be kept confidential and are not to be shared with other staff.

5.1.2.6 Access to USB ports and controllers on data entry computers are restricted and CD drives are disabled. File system access is also read-only. Database access is restricted to specific data entry software tools.

5.1.2.7 Computers are to be locked before leaving workstation. This automatically obscures any data displayed on the screen.
5.1.3 Visitors to the HIC Business Support Data Entry Office

5.1.3.1 Visitors will identify themselves to a Senior Business Support Administrator or designated deputy by ringing the bell at the door. They will be required to sign in the Visitors’ Book. A Senior Business Support Administrator, or designated deputy, will be responsible for the visitor while they are in the office.

5.1.3.2 On departure, the visitor will be required to sign out of the Visitors’ Book before exiting the office.

5.1.4 Staff Entry/Exit Procedures

5.1.4.1 Entry Procedures: Staff will be given the access code for the security door. This must not be shared with anyone and will be changed whenever a member of staff leaves employment.

5.1.4.2 Exit Procedures: At the end of the working day staff are required to ensure that all filing cabinets, windows and doors are locked, and lights are switched off.

5.1.5.3 Outside working hours: IT restrictions are in place for HIC Business support staff involved in data entry to ensure that they cannot login outside 08:00-18:00 Monday-Friday. This is to remove the risk that individuals could gain access after-hours to identifiable data.

6. APPLICABLE REFERENCES

- HIC Services SOP 06 Data Entry Training
- HIC Staff Confidentiality Agreement
- HIC Services SOP 07 Record of Custody
- HIC Services SOP 09 Data Entry Quality Control
- HIC Services SOP 01 HIC Data Security
- HIC Services SOP Appendix A – Policy
- HIC Services SOP Appendix B – Definitions
- HIC services SOP Appendix C – Roles and Contact Details