| | | | |
|---|---|---|---|
| Directorate | **Assurance and Risk Management** | Project | **Data Sharing Audits** |
| | | Status | **Final** |
| Director | **James Hawkins** | Version | **1.0** |
| Owner | **James Hawkins** | Version issue date | **11/02/2021** |

# NHS Digital Post Audit Review of Data Sharing Activities: Cardiff University - Centre for Trials Research

# 1 Audit Summary

## 1.1 Purpose

This report provides the formal closure of the data sharing audit at the Centre for Trials Research (CTR) at Cardiff University on 13 and 14 May 2019 against the requirements of the data sharing framework contract (DSFC) CON-311457-N2L9D and the data sharing agreement (DSA) DARS-NIC - 333498-D1K7G v3.8 with respect to the provision of:

| Dataset | Classification of Data | Dataset period |
|---|---|---|
| Hospital Episode Statistics (HES) Admitted Patient Care | Anonymised/Pseudonymised, Non-sensitive | 2009/10 – 2014/15 |
| HES Outpatients | Anonymised/Pseudonymised, Non-sensitive | 2009/10 – 2014/15 |
| HES Accident and Emergency | Anonymised/Pseudonymised, Non-sensitive | 2009/10 – 2014/15 |
| Office for National Statistics (ONS) Mortality Data | Anonymised/Pseudonymised, Sensitive | 2009/10 – 2014/15 |
| Bridge file: HES to Mortality Data from the ONS | Anonymised/Pseudonymised, Non-sensitive | N/A |

The Controller is Cardiff University and the Processor is Swansea University. The data is held in Swansea University's Secure Anonymised Information Linkage (SAIL) Databank that is hosted on the UK Secure e-Research Platform (UKSeRP).

Further guidance on the terms used in this post audit report can be found in version 2 of the NHS Digital Audit Guide.

## 1.2 Post Audit Review

This post audit review comprised a desk-based assessment of the action plan and supporting evidence supplied by CTR and Swansea University between December 2019 and September 2020.

Based on this post audit review all findings have been closed.

## 1.3 Updated Risk Statement

Based on the results of the post audit review the risk statement has been reassessed as shown in the following table.

| Original Risk Statement | Current Risk Statement |
|---|---|
| Critical | Critical |
| High | High |
| **Medium** | Medium |
| Low | **Low** |

## 1.4 Data Recipient's Acceptance Statement

Cardiff University has reviewed this report and confirmed that it is accurate.

## 1.5 Data Recipient's Action Plan

As NHS Digital has closed the nonconformities and the point for follow-up, no further action is required by the Audit Team. However, there are two observations still open and CTR should complete the actions against the findings.

## 1.6 Disclaimer

NHS Digital takes all reasonable care to ensure that this audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. NHS Digital cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

# 2 Status

Table 1 and Table 2 identify the 4 agreement nonconformities, 5 observations and 1 follow-up item raised as part of the original audit.

| Ref | Finding | Link to Area | Update | Designation | Status |
|---|---|---|---|---|---|
| 1. | Cardiff University confirmed to NHS Digital in previous communications that data supplied by NHS digital held on the file server, replication server and backup disk was encrypted to AES 256. However, at the audit, the Processor declared data was not encrypted.<br>The Audit Team noted that there are plans to invest in new hardware in July 2019 and the data will be encrypted going forward. | Access Control | The CTR provided screenshots which showed that the encryption settings have been enabled to AES 256. | Agreement nonconformity | Closed |
| 2. | Cardiff University does not have a formal Information Asset Register (IAR) though the information is captured in different documents. | Operational Management | The CTR provided a copy of the new University-wide IAR, which contains entries for all data received from NHS Digital.<br>The CTR also provided a copy of its Standing Operating Procedure (SOP) which details the process for ongoing monitoring of this IAR. | Agreement nonconformity | Closed |

| Ref | Finding | Link to Area | Update | Designation | Status |
|---|---|---|---|---|---|
| 3. | Evidence was shown to the Audit Team that access to the folder holding NHS Digital data was reviewed in May 2019. The Audit Team recommended that this review of access takes place on a regular basis (every three months) and is documented. | Access Control | The CTR provided a copy of its updated SOP for processing data provided by NHS Digital. The SOP now states access rights to the folders holding NHS Digital data should be reviewed every 3 months.<br>The CTR has also developed a template log to record when checks have been performed and any issues found with the named users to the folders. A copy of the template was provided to the Audit Team.<br>As the CTR does not currently hold any data supplied by NHS Digital on Cardiff University's servers, no data access checks are possible at this moment in time. Data previously held by the CTR has been deleted and the submitted certificate of destruction has been acknowledged by NHS Digital. | Observation | Open, but not for follow-up |
| 4. | Cardiff University should seek regular documented assurance from the Processor on the IT and IG controls in place to protect the data supplied by NHS Digital. This assurance should be shared with the Information Asset Owner (IAO) at Cardiff University. | Operational Management | The CTR provided a copy of its SOP for the assessment of external vendors and sub-contractors. The SOP outlines the process for ensuring sub-contractors or third-party vendors remain compliant. This includes the Quality Assurance team requesting documented assurances from vendors on a 2-year basis.<br>The CTR has also updated its SOP for the SAIL databank. The SOP describes how to set up access, responsibilities whilst accessing the databank, and removal of access at the end of the study. | Observation | Open, but not for follow-up |

| Ref | Finding | Link to Area | Update | Designation | Status |
|---|---|---|---|---|---|
| 5. | Cardiff University is undertaking a data flow exercise as part of the workplan for General Data Protection Regulation (GDPR). The University should ensure that this data flow exercise includes the data supplied under the DSA. | Operational Management | The CTR stated that the data flow exercise has been completed for all but one of the current active NHS Digital DSAs held with the University and has been incorporated into the IAR. Note, the exercise still to be done does not include data supplied under the DSA being audited. A copy of the new Cardiff University IAR was provided to the Audit Team. | Observation | Closed |
| 6. | The contract between Cardiff University and Swansea University was signed in 2016. The contract has not been reviewed to check if it is compliant with GDPR.<br>Cardiff University has developed a new data processing agreement which covers the Controller and Processor relationship in more detail, compliant with GDPR, though this has not been signed between Cardiff University and Swansea University for the work undertaken as part of the DSA. | Operational Management | The CTR provided a copy of the updated agreement between Cardiff University and Swansea University, signed in August 2019. The agreement has taken into consideration appropriate data protection legislation including GDPR. | Observation | Closed |
| 7. | An investigation was ongoing at the time of the audit at both Cardiff University and the Processor on the root cause and the lessons that can be learnt from an instance where there was a failure to delete data from all data touchpoints. | Data Destruction | The CTR confirmed it had received a copy of the incident response report from Swansea University in June 2019. The report identified the corrective actions and the preventive action required to ensure data is removed from all touchpoints.<br>The CTR provided a copy of the Certificate of Destruction signed by both Cardiff University and Swansea University which was sent to NHS Digital. The Certificate of Destruction has been reviewed and acknowledged by the NHS Digital. | Follow-up | Closed |

**Table 1: Nonconformities, Observations and point for follow-up - Cardiff University**

| Ref | Finding | Link to Area | Update | Designation | Status |
|---|---|---|---|---|---|
| 8. | Swansea University must include the data supplied under this DSA and held on its infrastructure on its IAR.<br>Depending on the outcome of the review of the failure to delete data from all data touchpoints, Swansea University may wish to include all the data touch point locations where the data is processed and stored, on the IAR. | Operational Management | The SAIL Data Management Group has updated its Terms of Reference to require the group to record and review NHS Digital information assets detailed within the SAIL IAR.<br>A screenshot was provided of the SAIL IAR with the filename 'Project 0301 – Building Blocks – Information Asset Register Entry'. | Agreement nonconformity | Closed |
| 9. | The Audit Team identified one user at Swansea University that had access to the data supplied by NHS Digital who had not completed IG training in the last 12 months. The DSFC requires all users with access to NHS Digital data to complete suitable training on an annual basis | Operational Management | A copy of the certificate to confirm that the user had undertaken and passed the Research, GDPR and Confidentiality test shortly after the audit was provided to the Audit Team. The training was provided by the Medical Research Council (MRC). | Agreement nonconformity | Closed |
| 10. | Swansea University plans to commission an independent third-party in the next 6 months to carry out a penetration test on the network infrastructure holding data supplied by NHS Digital. The last penetration test was carried out about two years ago.<br>It should be noted that the Swansea University carries out monthly vulnerability scans on the network including the servers holding NHS Digital data. | Access Control | Swansea University provided a copy of the report for an external penetration test undertaken in June 2019. The test did not identify any critical, high or medium issues. | Observation | Closed |

**Table 1: Nonconformities and Observation - Swansea University**