Directorate / Programme	**Data Dissemination Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Terry Hill**	Version	**1.0**
Owner	**Rob Shaw**	Version issue date	**19/01/2017**

NHS Digital Audit of Data Sharing Activities: School of Social and Community Medicine, University of Bristol

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at the School of Social and Community Medicine (SSCM), University of Bristol on 10 and 11 November 2016. It provides an evaluation of how the SSCM conforms to the requirements of the data sharing framework contract (DSFC) CON-304765-H4P3X and the data sharing agreement (DSA) NIC-30560-W4V1T with respect to the provision of:

Dataset(s)	"Level" of data	Dataset period
Hospital Episode Statistics - Admitted Patient Care for a cohort of about 50 records	Pseudonymised Non Sensitive	2002/03 to 2015/16

The report also considers whether the SSCM conforms to its own policies and procedures.

Between 2003 and 2006 the DRIFT (drainage, irrigation and fibrinolytic therapy) study recruited premature infants with post-haemorrhagic ventricular dilatation. Infants were randomised to receive a novel DRIFT treatment or standard therapy which consisted of lumbar punctures and if needed a ventricular reservoir to drain cerebrospinal fluid.

In 2014, the NIHR Health Technology Assessment programme funded the DRIFT research team (based at the University Hospitals Bristol and the University of Bristol) to conduct a long term follow up of children at school age.

The aims of this long term follow up were to:

- compare cognitive function, visual function, sensorimotor ability and emotional wellbeing between the two treatment groups in the DRIFT trial at school age;
- quantify functional status and use of community and specialist health and educational services;
- estimate the economic cost and outcomes of the DRIFT intervention by age 11 and model long-term costs and outcomes; and
- quantify degree of ventricular dilatation and neurosurgical sequelae in the two treatment groups by clinical neuroimaging.

To support the study, the University Hospitals Bristol sent identifiers and the DRIFT trial participant IDs to NHS Digital. NHS Digital used these identifiers to link to HES data for the cohort in the years since birth and returned this information identified purely by the DRIFT participant ID to the University of Bristol for analysis.

This is an exception report based on the criteria expressed in the NHS Digital Audit Guide.

1.2 Scope and Assurance Statement

The audit considered the fitness for purpose of the main processes with respect to data handling at the SSCM along with its associated documentation against the scope areas shown in Table 1.

The NHS Digital Audit Team has assigned the following assurance ratings to these areas based upon the findings of the audit.

Information Transfer	Limited assurance
Access Control	Moderate assurance
Data Use and Benefits	Moderate assurance
Risk Management	Substantial assurance
Operational Management and Control	Moderate assurance
Data Destruction	Moderate assurance

Table 1: Scope and Assurance rating

Detailed findings related to the areas of scope are detailed in Table 2.

1.3 Overall Risk Statement

It is the Audit Team's opinion that at the current time and based on evidence presented during the audit and the type of data being shared, there is a medium risk of a breach of information security, duties of care, confidentiality or integrity (including inappropriate access to or loss of data) provided by NHS Digital to the SSCM, University of Bristol under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

The SSCM has reviewed this report and confirmed that it is accurate.

The SSCM will establish a corrective action plan to address each finding shown in Table 2. The NHS Digital will validate this plan and the resultant actions at a post audit review with the SSCM to confirm the findings have been satisfactorily addressed.

2 Findings

Table 2 identifies 2 major nonconformities and 7 observations were raised as part of the audit.

In addressing a finding the data recipient must take account of any referenced supplementary notes.

Ref	Comments	Link to Area	Clause	Designation	Notes
1.	The DSA and System Level Security Policy (SLSP) do not reflect current practice and need to be corrected.	Access Control / Information Transfer	System Level Security Policy Data Sharing Agreement	Major	1
2.	The Audit Team found that the pseudonymised data supplied by NHS Digital was being linked to other data. The NHS Digital DARS team has confirmed that the linkage did not re-identify the data. This is a breach of the DSA section 5b, which states that 'the pseudonymised data supplied by NHS Digital will not be re-identified nor linked with the UHB's identifiable data or any other data.	Data Use and Benefits	Data Sharing Agreement clause 5b	Major	
3.	The incident reporting process is not documented. The SSCM should consider documenting the incident reporting procedures to including reference to NHS Digital guidance on incident reporting and timescales.	Operational Management		Observation	
4.	There was no documented procedure for the handling of NHS Digital data.	Operational Management		Observation	
5.	There has been no review of user access to the network folder holding NHS Digital data. It should be noted at the time of the audit, the SSCM had only had the data for two months and the Audit Team was informed that this check was planned. Ideally, this process should be documented in the procedure for handling NHS Digital data.	Access Control	Data Sharing Framework Contract Schedule 2, Section A, clause 1.2 and 4.1	Observation	
6.	The corporate or local Information Asset Register (IAR) did not include NHS Digital information assets. The IG policy supporting the IAR was being developed at the time of the audit and as a consequence this finding has been only raised as an observation.	Operational Management		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
7.	An Information Asset Owner (IAO) has been assigned for NHS Digital data. However the IAO has not completed specialist IAO training to support this role though has undertaken specific research training including handling NHS Digital data.	Operational Management		Observation	
8.	To complement the current external vulnerability test, the University of Bristol should consider penetration/vulnerability testing on the storage locations where NHS Digital data is held to ensure suitable controls are in place.	Access Management		Observation	
9.	To ensure adherence to the NHS Digital DSFC on permanent data deletion, the University of Bristol should consider the use of specialist software to ensure data is not recoverable. Furthermore the decommission of IT hardware with a footprint of NHS Digital needs to include a full audit trail to support the process.	Data Destruction		Observation	

Table 2: Nonconformities and Observations

2.1 Supplementary Notes

The following notes refer back to Table 2 and provide additional commentary on the linked finding.

Note 1. The DSA and System Level Security Policy (SLSP) do not reflect current practice and need to be corrected. Examples of inaccuracies are:

- the primary storage location is the University of Bristol datacentre and not Canynge Hall as stated;
- an additional backup disc based solution at the University of Bristol datacentre is not documented;
- the replication of raw and processed NHS Digital data to disc located at the University of West England is not documented;
- access to NHS Digital data is not locked down to specific PC by IP address. Access to the data is instead locked down by active directory user permissions;
- there is no encryption of the data at rest /storage on the primary cluster in the University of Bristol datacentre;
- the HES folder holding NHS Digital is not auditable (access logging) as stated in the SLSP. The data is logged however there are no tools to analysis the data at present; and
- no SQL server is used to hold or analysis NHS Digital data.

For the audit the SSCM had produced a list of necessary amendments to the SLSP, though this list did not include any information regarding backup to disc which was only identified during the audit.

2.2 Backup Retention

The duration for which data may be retained on backup media is shown in Table 3.

Backup retention	4 weeks (disc) 3 months (tape)

Table 3: Data Retention Period

2.3 Good Practice

In addition to the findings presented in Table 2 the Audit Team noted the following areas of good practice:

- The Project Lead has produced a report using the data provided which shows direct benefits to health and social care.
- The University is developing a range of corporate Information Governance policies.
- There is regular external vulnerability testing of the UoB IT infrastructure

2.4 Disclaimer

NHS Digital has prepared this audit report for its own purposes. As a result, NHS Digital does not assume any liability to any person or organisation for any loss or damage suffered or costs incurred by it arising out of, or in connection with, this report, however such loss or damage is caused. NHS Digital does not assume liability for any loss occasioned to any person or organisation acting or refraining from acting as a result of any information contained in this report.