Directorate / Programme	**Data Dissemination Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Terry Hill**	Version	**1.0**
Owner	**Rob Shaw**	Version issue date	**18/04/2017**

NHS Digital Audit of Data Sharing Activities: Leeds Teaching Hospitals NHS Trust

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at the Cardiology Department in Leeds Teaching Hospitals NHS Trust (LTH) on 9 and 10 January 2017. It provides an evaluation of how LTH conforms to the requirements of the data sharing framework contract (DSFC) CON-312951-B3L2Z and the data sharing agreement (DSA) NIC-148358-68V63 with respect to the provision of Office of National Statistics (ONS) death registrations details.

This data has been used to support the Space Rocket (Secondary Prevention of Acute Coronary Events. Reduction of Cholesterol to Key European Targets) research trial which conducted an open label comparative investigation of efficacy, tolerance and health in 2,072 consenting patients randomised to Rosuvastatin or 'standard' Simvastatin therapy following hospital admission for new definition myocardial infarction.

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

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 LTH 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	Moderate assurance
Access Control	Unsatisfactory assurance
Data Use and Benefits	Substantial assurance
Risk Management	Substantial assurance
Operational Management and Control	Moderate assurance
Data Destruction	Unsatisfactory 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 high 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 LTH under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

LTH has reviewed this report and confirmed that it is accurate.

LTH will establish a corrective action plan to address each finding shown in Table 2. NHS Digital will validate this plan and the resultant actions at a post audit review with LTH to confirm the findings have been satisfactorily addressed. The post audit review will also consider the outstanding evidence at which point the Audit Team may raise further nonconformities/observations.

2 Findings

Table 2 identifies the 2 major nonconformities, 4 minor nonconformities, 4 observations and 1 point for follow-up 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.	Access to the Space Rocket project folder is not being managed appropriately. A significant number of personnel not associated with the work were found to have access to this folder. No regular review of folder access is conducted to ensure that appropriate permissions are in force.	Access Control	DSFC, Schedule 2, Section, Clause 4.1	Major	1
2.	Assets awaiting disposal are retained in open trolleys in a secure corridor. No records are created of what is placed in the trolleys and eventually sent for destruction. Discs are not wiped before being placed in the trolley or taken by the third party recycling company.	Data Destruction	DSFC, Schedule 2, Section, Clause 4.10	Major	2
3.	Changes to named access to the ONS data have not been communicated with NHS Digital. *Notification of the latest change was initiated during the on-site visit.*	Access Control	DSA clause 6	Minor	
4.	IG training was not up to date for all relevant staff.	Operational Management	DSFC, Schedule 2, Section, Clause 1.3.2	Minor	
5.	Although LTH stated that the password policy was enforced by a 'Group Policy' no evidence of the configuration was provided. A screenshot supplied by LTH appeared to disagree with the Use of Computing Facilities Policy.	Access Control	DSFC, Schedule 2, Section, Clause 4.2 LTH, Use of Computing Facilities Policy, section 4.	Minor	
6.	No evidence was supplied to demonstrate that backups are suitably encrypted.	Access Control	DSFC, Schedule 2, Section, Clauses 4.5 and 4.7	Minor	
7.	Research projects do not fall within the remit of internal audit. The Trust is undertaking a review to ensure monitoring of contracts and agreements.	Operational Management		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
8.	There is no proactive information governance involvement in research projects to ensure that information governance / information security requirements are properly accounted for and that the Trust is able to fulfil any such obligations.	Operational Management		Observation	
9.	The information asset register is based around systems and not discrete elements, such as supplied ONS data.	Operational Management		Observation	
10.	A number of LTH documents have gone beyond their declared review date, for example, Use of Computing Facilities Policy, Research Governance Policy, Network and Network Client Security Policy and Remote Access Policy. It was stated by LTH that three policies had recently been rewritten and were awaiting approval by the Executive Team.	Operational Management		Observation	
11.	There is a need to resolve the retention of data with respect to research requirements and the disposal requirements of the agreement / contract.	Data Destruction	DSFC, Part 2, Clause 4.3.5	Follow-up	3

Table 2: Nonconformities, Observations and Points for follow-up

2.1 Supplementary Notes

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

Note 1. LTH provided a list of names that could access the project folder. When the Audit Team questioned the extensive nature of the list LTH recognised that almost 50 of the names presented in the list should not have access to the folder.

No defined joiners and leavers process was supplied to the Audit Team; only an Induction Policy was provided.

Note 2. Hard disc drives in desktops and servers are not encrypted; only laptops are encrypted. The Use of Computing Facilities policy states that “staff must not store confidential data on the hard disk or local drive of any computer”. However, it is unknown as to whether the SPSS application used to analyse the data stores temporary/cache files on the desktop drive.

No LTH branded disposal policy/procedure was provided to the Audit Team. Instead, a “Disposal Schedule” produced by the National Archives © 2012 was supplied.

No attempt to securely wipe data from redundant discs is undertaken by LTH prior to the asset being placed in the storage trolley.

Whilst an inventory list is received back from the third party company, no reconciliation is possible as LTH do not record what was placed within the trolleys.

The contracts held with the two third party recycling companies specify secure wiping before discs are resold or auctioned. Neither contract mentions crushing or shredding nor do they specify what action is to be taken in the event that a disc cannot be wiped. The special conditions at the back of the contracts with the two third party recycling companies are slightly different.

A copy of NHS Digital’s latest guidance on data destruction will be provided to LTH.

Note 3. LTH needs to establish what information is to be retained as part of the research project, given that records are also maintained by the Clinical Trial Research Unit (CTRU) at the University of Leeds. CTRU was not named on the original DSA signed in 2008, however LTH did provide an undated System Specific Security Policy which identified that the trial was sponsored by the University of Leeds and records were retained by the unit.

2.2 Backup Retention

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

Backup retention	Backups has been identified as a follow-up action due to data also being held by the CTRU at the University of Leeds; see Ref 11.

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 work is leading to benefits in health and social care; a number of articles were published in 2009 and 2010.

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.