Directorate / Programme	**Data Dissemination Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Terry Hill**	Version	**2.0**
Owner	**Rob Shaw**	Version issue date	**05/05/2017**

NHS Digital Audit of Data Sharing Activities: University College London – SLMS

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at the School of Life and Medical Sciences (SLMS) at University College London (UCL) on 7 and 8 February 2017 with respect to the British Women's Heart and Health Study. It provides an evaluation of how UCL conforms to the requirements of the data sharing framework contract (DSFC) CON-321538-B5D8B and the data sharing agreement (DSA) NIC-148101-R7RSL, including terms set out in letter of novation dated 10 August 2016, with respect to the provision of Office for National Statistics (ONS) data. The UCL study team is currently going through a renewal application. As part of the process UCL are reviewing security arrangements with NHS Digital.

UCL's Data Safe Haven platform is certified to ISO 27001:2013.

The report also considers whether UCL 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 UCL 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	Substantial assurance
Data Use and Benefits	Substantial 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. It should be noted that since the incident, which lead to the major nonconformity, was deemed to be an isolated incident and had been fully investigated and reported to the ICO through the SIRI tool in 2016 the above assurance ratings have been scored accordingly.

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 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 UCL under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

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

UCL 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 UCL 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 1 major nonconformity, 3 minor nonconformities, 16 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.	ONS data was released to a third party developer without prior approval from NHS Digital as required by the DSFC and DSA. UCL did however inform the ICO and NHS Digital of the data breach through the SIRI tool. UCL has provided an improvement plan to the ICO and is currently working through the defined actions.	Information Transfer	DSFC, Part 2, clause 4.3.3 DSA, clause 6	Major	1
2.	Actions and resulting changes to the network from the last penetration test could not be evidenced. The normal process within UCL is to provide a formal response to a penetration test. UCL stated verbally that some of the findings have been addressed.	Operational Management	DSFC, Schedule 2, Part A, clause 4.11	Minor	
3.	There is no complete corporate information asset register (IAR) which identifies NHS Digital data held. UCL acknowledged that the Data Protection Officer does not maintain a register for research projects.	Operational Management	UCL, Data Protection Policy, Paragraph 4	Minor	
4.	The training needs analysis document requires update to reflect current practice.	Operational Management	School of Life and Medical Sciences IG 16 Training needs analysis, Appendix 1	Minor	
5.	The IAR should contain the effective dates of contracts and agreements which could also contain links to other documents such as the information risk register.	Operational Management		Observation	
6.	UCL is conducting annual reviews of folder permissions. The Audit Team suggested that annual is too long and a more frequent review would be advisable.	Access Control		Observation	
7.	The collaboration spreadsheet should be updated to include date of information transfer.	Information Transfer		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
8.	Principal Investigators (PIs) may not have ready access to all contractual material even though there maybe information governance / information security obligations contained within the material.	Operational Management		Observation	
9.	UCL to record evidence of future data destruction, for example screenshot of Cipher if this is the approach to be taken. This approach has been discussed with NHS Digital as part of the current application.	Data Destruction		Observation	
10.	The physical risk assessment has not been fully completed for study. The Audit Team questioned the value being added to the overall risk assessment process that it currently gives.	Risk Management		Observation	
11.	A Standard Operating Procedure for handling NHS Digital data should be implemented for the organisation.	Operational Management		Observation	
12.	Specific study training is provided to recognise differing demands around NHS digital supplied data, for example ONS and HES.	Operational Management		Observation	
13.	UCL to consider how Privacy Impact Assessments becomes embedded with its standard operating model.	Operational Management		Observation	
14.	The collaboration request form to include a field asking whether the requested data includes personal confidential information.	Operational Management		Observation	
15.	Inform those using the Managed File Transfer facility to send data that if they realise the wrong file has been attached that IT can remove the file potentially before it is downloaded by the recipient.	Information Transfer		Observation	
16.	Documentation management information to be improved as some details are incorrect, for example, the IG Policy.	Operational Management		Observation	
17.	UCL to implement a mechanism to inform staff of changes to key policies and processes.	Operational Management		Observation	
18.	The PI is involved in agreeing the level of data to be supplied to collaborators but there is no independent check of the accuracy of the output. For this study the database from which evidence is extract does not contain original ONS data.	Information Transfer		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
19.	Published reports to acknowledge use of NHS Digital data where appropriate.	Data Use and Benefits		Observation	
20.	Some of the information raised during the audit which talks about parties who have had access to the data and an analysis of why the data could not be reidentified should be sent to DARS as additional information and in one case correct previously supplied information.	Data Use and Benefits		Observation	
21.	UCL to clarify the position around the return of failed discs under warranty to manufacturers or obtain written statement from manufacturer. No record of returned discs is kept.	Data Destruction		Follow-up	

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. During the course of the audit UCL identified a data breach that had occurred in 2016 related to data that had been supplied by NHS Digital.

A copy of a database containing sensitive data was sent to a third party developer in order for the developer to provide support on the database under a non-disclosure agreement. NHS Digital was not informed of the use of the third party.

A comprehensive investigation was undertaken by UCL following the incident being raised internally. The investigation concluded the developer did not need the data to do the work and was requested to irretrievably destroy the data. The Audit Team did not see evidence from the third party developer which confirmed data destruction.

The data breach was reported through the SIRI tool at the time of the investigation. From this submission the ICO asked UCL to set out an improvement plan to address the issues highlighted by the investigation. UCL are currently undertaking these actions.

2.2 Backup Retention

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

Backup retention	Tapes - 90 days

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:

- a considerable number of publications has been produced from the research; and
- the data safe haven environment provides a secure repository which is certified to ISO 27001:2013.

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.