

Directorate / Programme	Care Services	Project	Data Sharing Audits
		Status	Approved
Director	Catherine O’Keeffe	Version	1.0
Owner	Sean Walsh	Version issue date	11/08/2017

NHS Digital Audit of Data Sharing Activities: Nottinghamshire County Council – Public Health

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at Nottinghamshire County Council (NCC) Public Health (PH) on 29 and 30 June 2017. It provides an evaluation of how NCC conforms to the requirements of the data sharing framework contract (DSFC) CON-389496-S4N5H and the data sharing agreement (DSA) DARS-NIC-389495-J7Z8L with respect to the provision of the following Hospital Episode Statistics (HES) datasets:

HES Dataset	Level of data	Dataset period
Admitted Patient Care	Pseudonymised /Anonymised Non Sensitive	2016-2017 (M11 to M13 including AR) 2017-2018 (M2 to M10)
Outpatients	Pseudonymised /Anonymised Non Sensitive	2016-2017 (M11 to M13 including AR) 2017-2018 (M2 to M10)
HES Accident and Emergency	Pseudonymised /Anonymised Non Sensitive	2016-2017 (M11 to M13 including AR) 2017-2018 (M2 to M10)

Table 1: DSA Datasets

The above datasets supplement previous years already held by the Council.

The data controller is NCC and the data processor is Nottinghamshire Health Informatics Service (NHIS). NHIS is certified to ISO 27001:2013 for IT support.

The report also considers whether NCC 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 NCC along with its associated documentation against the scope areas shown in Table 2.

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 2: Scope and Assurance rating for NCC

Detailed findings related to the areas of scope are detailed in Table 3.

1.3 Overall Risk Statement

It is the Audit Team's opinion that based on evidence presented during the audit and the type of data being shared, there is low 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 NCC under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

NCC PH has reviewed this report and confirmed that it is accurate.

NCC PH will establish a corrective action plan to address each finding shown in Table 3. NHS Digital will validate this plan and the resultant actions at a post audit review with NCC to confirm the findings have been satisfactorily addressed.

2 Findings

Table 3 and Table 4 identify the minor nonconformities, observations and item for follow-up raised as part of the audit for NCC and NHIS respectively. NCC will be responsible for reporting on the findings raised against NHIS.

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

Ref	Comments	Link to Area	Clause	Designation	Notes
1.	NHS Digital data is being processed and stored at locations that are not declared on the DSA, namely the NCC DR site and the NHIS data centre. Although the NCC DR site is not council owned, the equipment is and is maintained by council staff.	Information Transfer	DSA, 2a and 2b	Minor	
2.	Training for certain NCC PH staff has not been renewed in the last year as the corporate policy states every two years.	Operational Management	DSFC, Schedule 2, 1.3.2	Minor	
3.	No Privacy Impact Assessment (PIA) has been undertaken by NCC for the NHS Digital data. It is NCC practice to complete at least the Part 1 to assess if a full PIA is required.	Operational Management	NCC, Guide to Privacy Impact Assessments	Minor	
4.	Whilst NCC and NHIS were very open during the on-site visit and provided a range of evidence, NCC refused to give the Audit Team sight of the vulnerability (NESSUS) / penetration testing and associated remediation plan(s) citing that it had provided the current Public Services Network (PSN) certificate.	Operational Management	DFSC, Part 2, 7.4	Minor	
5.	NCC should ensure that the appropriate teams have seen the DFSC and DSA to ensure the organisation is fully compliant. This is particularly the case of those DSA covering the provisions of ONS (Office of National Statistics) data.	Operational Management		Observation	
6.	NCC should produce a document which sets out the obligations of NHIS as the Data Processor, including any pertinent requirements in NCC's DSFC/DSA.	Operational Management		Observation	
7.	Incident reporting is under review. As part of this review NCC should ensure that the need to inform NHS Digital of any data / contract breach is reflected.	Operational Management	DSFC, 5.7	Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
8.	NCC needs to review its data deletion policy to ensure that any NHS Digital supplied data is permanently destroyed when no longer needed. As PH staff use Outlook and Outlook Web Access (OWA) as a mechanism to transfer data between NHIS and NCC networks, NCC needs to recognise that NHS Digital data has a footprint on its Exchange server. <i>The Audit Team provided a copy of NHS Digital's latest guidance.</i>	Data Destruction	DSFC, 4.3.5	Observation	
9.	Guidance should be developed by NCC around the handling and processing of NHS Digital data to provide consistency, including recognition of the various touch points.	Operational Management		Observation	
10.	Site visits should be undertaken by NCC to ensure that contracted third parties are discharging their activities appropriately.	Operational Management		Observation	
11.	The Audit Team is to review further evidence associated with the destruction lifecycle of hardware, namely PCs and laptops.	Data Destruction		Follow-up	

Table 3: NCC – Nonconformities, Observations and Point for follow-up

Ref	Comments	Link to Area	Clause	Designation	Notes
12.	NHIS needs to review its media deletion practices to ensure that any NHS Digital supplied data is permanently destroyed from its systems when no longer needed. This will include both the raw HES files and the database tables.	Data Destruction	DSFC, 4.3.5	Observation	
13.	NHIS should review its access control policy to consider whether the annual review for ensuring correct access is too infrequent.	Access Control	NHIS, Logical Access Control Policy, 7.7	Observation	
14.	NHIS should review its external approval process to ensure that it only processes requests for data access from known NCC managers.	Access Control		Observation	

Table 4: NHIS - Observations

2.1 Supplementary Notes

Not Applicable.

2.2 Data Location

NCC confirmed that processing and storage, including disaster recovery and backups, of the data was limited to the location shown in Table 5.

Data Location	England
---------------	---------

Table 5: Data Location

2.3 Backup Retention

The duration for which data may be retained on backup media is shown in Table 6.

Backup retention	NCC		30 days	
	NHIS	File server	Daily	14 days
			Weekly	28 days
			Monthly	365 days
			Yearly	5 Years
		Database Server DB	Daily	4 days

Table 6: Data Retention Period

2.4 Good Practice

In addition to the findings presented in Table 3 the Audit Team noted the following areas of good practice:

- NCC is actively reviewing its practices to ensure their fitness for purpose
- The council demonstrated clear benefits to health and social care
- There are reasonable physical controls at the NCC datacentre that was visited during the audit.

2.5 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.