Directorate / Programme	**Care Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Catherine O'Keeffe**	Version	**1.0**
Owner	**Rob Shaw**	Version issue date	**25/04/2018**

NHS Digital Audit of Data Sharing Activities: Gateshead Metropolitan Borough Council

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at Gateshead Metropolitan Borough Council (GMBC) on 25 and 26 January 2018. It provides an evaluation of how GMBC conforms to the requirements of the data sharing framework contract (DSFC) CON-387343-C7Q1Z version 2.01 and the data sharing agreement (DSA) NIC-31865-Z2Y1D-version 2.2 with respect to the provision of:

Hospital Episode Statistics (HES) Dataset	Classification of Data	Dataset period
HES - Admitted Patient Care	Anonymised/Pseudonymised, Non-Sensitive	2006/07 – 2017/18
HES - Outpatients	Anonymised/Pseudonymised, Non-Sensitive	2006/07 – 2017/18
HES - Accident and Emergency	Anonymised/Pseudonymised, Non-Sensitive	2006/07 – 2017/18

The HES datasets are accessed through the HES Data Interrogation System (HDIS). The DSA allows the two registered HDIS users to download record level data from the system.

The Data Controller is GMBC.

The report also considers whether GMBC conforms to its own policies, processes and procedures.

This is an exception report based on the criteria expressed in the NHS Digital Audit Guide version 2.0.

1.2 Type of Audit and Audit Scope

Audit type	Routine
Scope areas	Information Transfer Access Control Data Use and Benefits Risk Management Operational Management and Control Data Destruction

At the time of the audit, the Council only had accessed the HES data in December 2017 and had no outputs completed for the Audit Team to review against the DSA.

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, the following 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 under the terms and conditions of the data sharing agreement signed by both parties has been assigned.

Critical Risk
High Risk
Medium Risk
Low Risk

1.4 Response

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

GMBC 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 GMBC to confirm the findings have been satisfactorily addressed.

2 Findings

Table 1 identifies the 3 agreement nonconformities, 2 organisation nonconformities and 8 observations that were raised as part of the audit.

In addressing a finding the data recipient must take account of any referenced supplementary notes in section 2.1.

Ref	Comments	Link to Area	Clause	Designation	Notes
1.	The Council has not destroyed HES data supplied under a previous DSA and has not supplied NHS Digital with a data destruction certificate by the 30 June 2017, as stated in the special conditions of the current DSA (although the Council did request advice from NHS Digital to do this in May 2017, which was not forthcoming). The current DSA was signed by the Council in July 2017.	Data Destruction	DSA, Annex A, Section 6 (Special Conditions)	Agreement nonconformity	Note 1
2.	The Council is storing NHS Digital data at a location which is not declared in the DSA. The missing address is a Council owned building.	Information Transfer	DSA, Annex A, Section 2b	Agreement nonconformity	
3.	There was no evidence to show that user permissions to the network folder holding the NHS Digital data had been reviewed on a regular basis. The Council's Information Security Strategy section 2.6.2 states "Formal procedures should be in place to control the allocation of access rights to information systems and services. These access rights should be reviewed on a regular basis and revised as necessary".	Access Control	GMBC, Information Security Strategy, Section 2.6	Organisation nonconformity	

Ref	Comments	Link to Area	Clause	Designation	Notes
4.	The Council has a Public Health Information Asset Register (IAR) however it did not include an entry for the HES datasets supplied by NHS Digital. The DSA identifies the Information Asset Owner (IAO) as the Director of Public Health. The Council complete the Information Governance Toolkit (IGT) to support provide security assurance for the DSFC. IGT requirement 381 - 'A list of information assets has been compiled in a register which includes the location and 'owner' for each asset'. At level 2a requires 'All information assets have been documented in a register that includes relevant details about each asset (i.e. the location of each asset, what type of information, who uses it etc)'. The Council self-assessed as level 2 compliant in 2016/17. The Council also have the role of Information Asset Assistant (IAA) to support the IAO and this could be included recorded on the IAR. Logging of the asset on the IAR may also help to ensure that specialist training to support the IAO and IAA is provided, risk assessments for the data asset are completed and formal logging of the information classification for this asset.	Operational Management	DSFC, Schedule 2, Section A, Clause 3.2. DSFC, Part 2, Clause 4.1.3	Agreement nonconformity	
5.	A number of documents provided as part of the pre-audit documentation need to be reviewed and updated. This includes adding version history to documents as required by the Information Management Strategy, Section 8.3.	Operational Management	GMBC, Information Management Strategy, Section 8.3. GMBC, Risk Management Policy, Section 5 GMBC, ICT Security Policy	Organisation nonconformity	Note 2
6.	At the time of the audit, the Council did not have a Public Service Network (PSN) connection compliance certificate due to the number of recorded internal vulnerabilities. The Council did, however, have an active resolution process and was confident that the recorded actions would be completed by the end of February 2018.	Access Control		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
7.	The Council uses Microsoft Excel installed on desktop PCs to process the HES data. If Excel experiences an abnormal shutdown the application creates temporary files in a temporary path folder on the network file storage. The Audit Team checked the folder and found it contained a number of files however none of these contained HES data. The Council should ensure that appropriate controls are put in place to remove and control access to any such files.	Access Control		Observation	
8.	It was reported that domain administrator / elevated privilege access is audited on an annual basis regular basis. The Audit Team suggested that this review is carried out on a more regularly basis and the management of these accounts is documented.	Access Control		Observation	
9.	The DSFC requires all users with access to NHS Digital data to complete suitable training on an annual basis. The Council were not able to provide training records for the two users that had access to NHS Digital data, however the trainer was able confirm that the users completed face to face data protection training on the 28 June 2017 from an entry in the Outlook Calendar. This was confirmed by the users as well. A copy of the training material was shared with the Audit Team. The Council confirmed that a new e-training system with a module covering information governance is now in place and is being rolled across the Council. This system will log training records.	Operational Management		Observation	
10.	The Council completes the Information Governance Toolkit (IGT) on an annual basis to provide security assurance to support the DSFC. It was noted that currently there is no independent assurance on the evidence and scores prior to the final IGT submission. The Audit Team suggested an independent audit by the Council's internal audit team is undertaken in January prior to submission in March.	Operational Management		Observation	
11.	The Council should ensure that the appropriate teams have seen the DSFC and DSA to ensure the organisation is aware of its obligations.	Operational Management		Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
12.	The Council should consider developing some guidance on the handling and processing of NHS Digital data. This guidance could include: • a data flow diagram which outlines all touch points for NHS Digital data; • regular review of access to folders containing NHS Digital data; • a section on data destruction, including the use of specialist software to ensure permanent deletion of data and a reference to Data Access Request Service (DARS) guidance on data deletion; • a section which outlines quality checks on outputs to ensure their accuracy including the source of the datasets.	Operational Management		Observation	
13.	Whilst IT equipment holding data is degaussed by the Council and crushed by a third-party disposal contractor at the Council's site, the asset serial number and the third-party's certificate of destruction are not reconciled to ensure both lists are consistent and to account for all assets.	Data Destruction		Observation	

Table 1: Nonconformities and Observations

2.1 Supplementary Notes

The following notes refer to Table 1 and provide additional commentary on the linked finding.

Note 1. The data in question, was downloaded monthly between June and December 2016. The Council soon realised that a SQL server would be needed to process the HES dataset, due to the size of the files. The Council was reluctant to invest in a SQL server due to potential cost and because members of the Public Health Intelligence North East (PHINE) Network were investigating the potential for a regional solution e.g. one authority hosting an SQL database on behalf of others. It should be noted that the Council confirmed that even though the files were downloaded, the datasets have never been opened.

Early in 2017, the Council requested advise about data deletion from the Data Access Request Service (DARS) team verbally and followed this up by email in May 2017, following review of NHS Digital's data destruction guidance. The Council was concerned that by using specialist data deletion software to securely wipe NHS Digital data from the network file storage, it may put other Council data at risk. Therefore, the Council felt that it could not delete the data without further advice, which was not forthcoming.

An email trail between the Council and the DARS team from May 2017 where the Council requested specialist advice from the DARS team on two occasions by email and indicated in the email that they had previously requested advice by telephone, was reviewed by the Audit Team. There was no evidence supplied to show any further communication between both parties regarding data destruction since the Council's final email request for assistance on 30 May 2017 and the DARS team's subsequent confirmation on 31 May 2017 that they would pursue the query and get back to the Council with a solution.

The current DSA covers the period from April 2017 until March 2018. The DSA was signed by the DARS team in June 2017 and by the Council in July 2017. The DSFC version 2.01 was signed by both parties in October 2017.

The Audit Team supplied a copy of the data destruction guidance, a blank copy of the certificate of destruction and contact details for the DARS Security Consultant to the Council.

During the audit, the Audit Team identified four storage touch points for NHS Digital data that the Council needs to consider when completing the Certificate of Destruction. The Audit Team advised the Council to seek further guidance NHS Digital, prior to any action being taken, so a solution which is acceptable to both parties can be agreed.

Note 2. Documents include:

- Risk Management Policy
  - The policy has an approval date of May 2013. Section 5 states the policy should be review on annual basis.
- Information Management Strategy
  - Section 8.3 states that documents will use a cover page and include version history to ensure tracking of document. The strategy document does not have a date of approval, approval body and next review date.
  - Refers to an Information Governance Working Group which does not exist.
- Information Security Strategy
  - Refers to version 1.0 and approval date 2005. The ICT lead did confirm that this document had been reviewed and logged on an internal spreadsheet, however a user would not be aware of this as there is no version history.

2.2 Use of Data

GMBC confirmed that the data was only being processed and used for the purposes defined in the DSA and was not being linked with another dataset.

2.3 Data Location

GMBC confirmed that processing and storage, including disaster recovery and backups, of the data was limited to the location shown in Table 2. This location conforms with the locality defined in clause 2c of the DSA.

GMBC	England

Table 2: Data Location

2.4 Backup Retention

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

Organisation	Media Type	Period
GMBC	Backup disk	28 days

Table 3: Data Retention Period

2.5 Good Practice

In addition to the findings presented in Table 1 the Audit Team noted the following areas of good practice:

- The Council confirmed that a new e-training system with a module covering risk management and information governance is now in place and is being rolled across the Council.

2.6 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.