Directorate / Programme	**Care Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Catherine O'Keeffe**	Version	**1.0**
Owner	**Rob Shaw**	Version issue date	**04/01/2018**

NHS Digital Post Audit Review of Data Sharing Activities: Vanguard - Moorfields Eye Hospital NHS Foundation Trust

1 Audit Summary

1.1 Purpose

This report provides the formal closure of the data sharing audit of Moorfields Eye Hospital NHS Foundation Trust (MEHFT) on 4 and 5 July 2017 against the requirements of the data sharing framework contract (DSFC) CON-313063-L9X6F and the data sharing agreement (DSA) NIC-15281-W8L6H with respect to the provision of:

Hopital Episode Statistics (HES) Dataset	Classification of data	Dataset period
Outpatients	Pseudonymised / Anonymised Non Sensitive	2010-2011; 2011-2012; 2012-2013; 2013-2014; 2014-2015
Admitted Patient Care	Pseudonymised / Anonymised Non Sensitive	2010-2011; 2011-2012; 2012-2013; 2013-2014; 2014-2015

The data controller is MEHFT and the data processor is NHS South, Central and West Commissioning Support Unit (CSU). The data was requested by MEHFT for the Vanguard project.

Further guidance on the terms used in this post audit review report can be found in the NHS Digital Audit Guide.

1.2 Post Audit Review

This post audit review comprised an assessment of the action plan and supporting evidence supplied by MEHFT during the onsite visit on 19 October 2017 and additional information supplied by email.

Based on this post audit review all findings have been closed.

1.3 Updated Risk Statement

In summary, it is the Audit Team's opinion that at the current time and based on evidence presented during the post audit review 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 MEHFT under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

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

As NHS Digital has closed all of the findings, no further action is required by MEHFT.

1.5 Disclaimer

NHS Digital takes all reasonable care to ensure that this audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. NHS Digital cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

2 Status

Table 1 (MEHFT) and Table 2 (CSU) identifies the three major nonconformities, four minor nonconformities and two observations raised as part of the original audit.

Ref	Comments	Link to Area	Update	Designation	Status
1	The raw HES data and the generated database tool (aggregated data) was transferred by the NHS South, Central and West Commissioning Support Unit (CSU) to MEHFT in May 2017 via a cloud based computer file transfer service, 'WeTransfer', which is founded in Amsterdam. The two issues arising from this transfer are: • An extract from the WeTransfer website regarding the location of their servers: 'To make sure we can offer the best and smoothest up- and download experience to all of you, we have servers both in the EU and the US. Where your transfer is stored depends on a couple of things: If you are in the EU when you upload the transfer; if the IP address you're using is European, and if you are not using an anonymous proxy..... we will store your data on our servers in the EU. We do however reserve the right to redirect your transfers to our US servers, in case there's no way to store them in the EU.' • The DSA only allows the holding of the raw data at the CSU's storage location. The Vanguard Project Lead has reported the incident internally to MEHFT's information governance department, who were unaware of the nature of the transfer. The Audit Team have advised MEHFT to report the incident to the	Information Transfer	The incident was reported internally by MEHFT and investigated by the Trust's Information Governance (IG) team. The incident was also reported to NHS Digital by MEHFT in July 2017. However it was noted by the Audit Team that the data type was reported as aggregated data instead of pseudonymised / anonymised data. Following identification, the incident report was updated and reported again to NHS Digital in October 2017 with the correct information. The Data Access Request Service (DARS) team requested MEHFT to complete a certificate of destruction for the raw data transferred via WeTransfer. MEHFT contacted WeTransfer to establish where the data was stored and its data deletion process. WeTransfer stated the data was held on servers in the European Union (EU) and the data is 'scrubbed' from the servers after seven days. However, the Certificate of Destruction submitted by MEHFT containing the responses from WeTransfer was rejected by the DARS team due to insufficient assurance. The following information was provided by the DARS team to explain their decision: WeTransfer is built on Amazon Web Services (AWS). There is no procedure to permanently remove the data from AWS. A file if flagged for deletion will be simply overwritten after an indeterminable amount of time but there is no verification available. It is therefore possible that the data is still present on the server. AWS do however encrypt the data to the NHS standard and as a further security measure encrypt the key. This level of encryption would	Major	Closed

Ref	Comments	Link to Area	Update	Designation	Status
	DARS team as this is a breach of the DSA.		mean that there would be a low risk of a data breach. This point is further mitigated as the data is pseudonymised / anonymised. No further action is planned by the DARS team.		
2	The CSU has been processing and storing NHS Digital data at locations which are not stated in the DSA. MEHFT has been storing NHS Digital data at locations which are not stated in the DSA. This includes downloading the data onto a Trust PC and MEHFT network drive. The original HES zip files was downloaded by MEHFT from WeTransfer and unzipped onto an unencrypted Trust PC. The unzipping process may have created temporary files on the local drive. The raw files were then copied onto the MEHFT's network file storage and the copies of the files in the PC download folder were deleted through a logical delete. MEHFT's IT Team needs to determine how it will securely destroy the data once the DSA comes to an end; this will include the drive on the PC and its network storage. Please note that MEHFT confirmed that outside of the CSU, the raw HES data has not been shared with any other third parties.	Information Transfer	MEHFT has supplied the DARS team with details of the four storage locations (two MEHFT and two CSU locations) where the raw data was stored, including backups. Following the audit in July 2017, the DARS team requested that the data was deleted in line with NHS Digital guidance. The DARS team has accepted the Certificate of Destruction completed by MEHFT for its internal storage locations.	Major	Closed

Ref	Comments	Link to Area	Update	Designation	Status
3	There is no written agreement in place identifying the roles and responsibilities between MEHFT and CSU as the work was commissioned and instructed through a third party consultant. There was no written agreement between the consultant and MEHFT, so the consultant was unaware of the requirements of the DSA and DSFC. The consultant also forwarded the database tool produced by the CSU to another third party consultant to update a market report for MEHFT. There is no reference in the DSA on the use of third party consultants.	Operational Management	MEHFT has acknowledged that the following documentation should have been completed prior to signing the DSA as a minimum: • a confidentiality agreement signed by all third-parties; and • an information security third-party checklist. The Audit Team also added that all third-parties involved in storing and processing NHS Digital data need to be declared on the DSA. Following the audit in July 2017, the DARS team requested that the database tool be deleted in line with NHS Digital guidance. It was identified the database tool, which was shared with two third-party consultants, contained aggregated data, however, small numbers had not been supressed in line with NHS Digital guidance. The two third-party consultants were requested by the DARS team to delete the database tool in line with NHS Digital guidance. The DARS team has accepted the Certificates of Destruction provided by the two third-party consultants. It was report that the Trust's Chief Executive Officer has requested that: • a paper is shared with the management executive team on lessons learnt from the audit; • the learning to be shared as a case study as part of the Moorfields IG toolkit training; and • a communication is sent to all staff following the re-audit with key reminders about the data request process; specifically signposting key policies and the need to involve IG staff when considering making any external data request.	Major	Closed

Ref	Comments	Link to Area	Update	Designation	Status
4	No risk assessment and Privacy Impact Assessment (PIA) had been carried by MEHFT on the data provided by NHS Digital.	Risk Management	MEHFT has discussed internally the risk associated with pseudonymised data in detail. It has acknowledged that an information security checklist should have been completed at the start which would have resulted in the pseudonymised data being classified as confidential. This classification would have triggered a PIA to be undertaken. MEHFT has decided it is not appropriate to complete a PIA since the data has now been deleted.	Minor	Closed
5	The data asset had been added onto the information asset register one day prior to the onsite audit. The Information Governance department had not completed an assessment to check the entry. No protective marking had been applied to the data assets in line with Trust guidance. The Information Asset Owner (IAO) had not completed specialist training required for the role.	Operational Management	MEHFT acknowledged that the information asset register owner was unaware of the NHS Digital data asset. An entry was only added to the Information Asset Register (IAR) following MEHFT's review of NHS Digital's Audit Guide. The Audit Team can confirm that the entry on the IAR is now completed. The Trust confirmed that it does not use protective marking as all information assets listed on the IAR are classed and treated as confidential. It was reported that specialist training is currently being rolled out to all IAOs. Although the NHS Digital data asset has now been deleted, the IAO may still need to undergo training if assessed as requiring training by the Trust.	Minor	Closed
6	The appropriate teams within MEHFT have not seen the DSA or the DSFC, so are unaware of the obligations to meet.	Operational Management	Following the original audit in July 2017, the DSA and DSFC have been shared with the IG team. The IG team has also requested a list of all ongoing data sharing applications with NHS Digital. The team also plan to devise a process to manage such applications going forward. The Audit Team advised MEHFT that future DSAs and DSFCs should be shared with IG and IT leads to ensure that requirements can be met prior to signing.	Observation	Closed

Table 1: Nonconformities and Observations - MEHFT

Ref	Comments	Link to Area	Update	Designation	Status
7	The Audit Team viewed the database tool which was developed by the CSU using the HES data. It was found that small numbers had not been suppressed in line with requirements in the DSA. The CSU had not received or seen the DSA. MEHFT also reported that they generally suppressed numbers below 10.	Data Use and Benefits	Following identification that small numbers had not been supressed, MEHFT sent the tool back to the CSU. The CSU was requested to supress small numbers below 10 in line with MEHFT internal practice. The Audit Team confirmed that small numbers had been supressed in the revised tool.	Minor	Closed
8	There was no evidence to show that access to the network folder holding the HES data at the CSU's site had been reviewed on a regular basis.	Access Control	The CSU confirmed that following the audit it carried out a review of the permissions for the network folder that held the raw data. It should be noted that at this point in time, the raw data had already been deleted. The review identified that three users had left the CSU, but their access had not been disabled. This has now been addressed by the CSU.	Minor	Closed
9	The raw data has been deleted by the CSU, which was held in two locations (file network storage and SQL server). However the data on the file network storage was deleted through a logical delete. The SQL database that contained the imported data was deleted by dropping the table. This data could be potentially recovered. The data has not been deleted from the backup locations. MEHFT should instruct the CSU to delete the data in accordance with the requirements of the DSFC.	Data Destruction	Following the audit in July 2017, the DARS team requested that the data was deleted in line with NHS Digital guidance. The Certificate of Destruction completed by the CSU has been accepted by the DARS team.	Observation	Closed

Table 2: Nonconformities and Observations - CSU