Directorate	**Assurance and Risk Management**	Project	**Data Sharing Audits**
		Status	**Final**
Director	**James Hawkins**	Version	**1.0**
Owner	**James Hawkins**	Version issue date	**21/12/2020**

NHS Digital Post Audit Review of Data Sharing Activities: East Staffordshire Clinical Commissioning Group

1 Audit Summary

1.1 Purpose

This report provides an update on progress of the data sharing audit of the East Staffordshire Clinical Commissioning Group (ESCCG) on 10 and 11 July 2018 against the requirements of the data sharing framework contract (DSFC) CON-391003-G4M0R v2.01 and the data sharing agreement (DSA) NIC-041540-K2N7Z v0.2 with respect to the provision of:

Dataset	Classification of Data	Dataset period
SUS (Invoice Validation and Risk Stratification) for commissioning	Identifiable Data, Sensitive	01/04/2013 - 27/06/2018
Improving Access to Psychological Therapies	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Diagnostic Imaging Dataset	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Mental Health Learning Disability Data Set	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Maternity Services Dataset	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Children and Young People's Health	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Acute-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Ambulance-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Community-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Demand for Service-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Diagnostic Services-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Emergency Care-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Experience, Quality and Outcomes-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Mental Health-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Other Not Elsewhere (NEC)-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Population Data-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Primary Care Services-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018

Public Health and Screening Services-Local Provider Flows	Pseudonymised/Anonymised, Sensitive	01/04/2013 - 27/06/2018
Mental Health Minimum Dataset	Pseudonymised/Anonymised, Sensitive	01/04/2013 – 31/03/2014
Mental Health and Learning Disabilities Dataset	Pseudonymised/Anonymised, Sensitive	01/04/2014 – 31/12/2015

Further guidance on the terms used in this post audit report can be found in version 2 of 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 the ESCCG between December 2019 and August 2020. It involved a desk-based review of evidence and telephone conversation. Additional supporting evidence was supplied via email following the telephone call.

From this post audit review 1 agreement nonconformity, 1 organisational nonconformity, 3 observations remain open and require further follow-up by the Audit Team.

Findings 1 and 22 have been assigned a finding status of 'Unresolved'. It is the Audit Team's view that no further action can be taken by the ESCCG as there is no contractual relationship between the ESCCG and Virgin Care, however, as the actions have not been completed, the findings cannot be closed. Should the ESCCG re-engage Virgin Care to process the data held under this DSA, then NHS Digital assumes the right to change the statuses back to Open.

1.3 Updated Risk Statement

Based on the results of the post audit review the risk statement has been reassessed as shown in the following table.

Original Risk Statement	Current Risk Statement
Critical	Critical
High	**High**
Medium	Medium
Low	Low

1.4 Data Recipient's Acceptance Statement

The ESCCG has reviewed this report and confirmed that it is accurate.

1.5 Data Recipient's Action Plan

The Audit Team found that the ESCCG has not suitably addressed all the nonconformities or outstanding points contained in the original data sharing audit report and further work is required to close those findings. The ESCCG is required to update its action plan to align with this post audit report.

1.6 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

Tables 1, 2 and 3 identify the 7 agreement nonconformities, 8 organisation nonconformities, 5 observations and 2 points for follow-up raised as part of the original audit.

The tables have introduced a new finding status of 'Unresolved', as no further action can be taken by the ESCCG but such findings cannot be closed. The use of Unresolved makes a distinction to those findings classed as Open where the Audit Team expects the organisation to suitability address them.

Ref	Finding	Link to Area	Update	Designation	Status
1.	Failure to secure access for the NHS Digital Audit Team into Virgin Care as required by the DSFC, despite a number of attempts being made by the Audit Team over several weeks to arrange an audit with Virgin Care.	Operational Management	In June 2019, the ESCCG terminated its contract with Virgin Care and processing ended around September 2019. At which point the ESCCG asked Virgin Care to delete the data, but Virgin Care declined. The Audit Team has subsequently been informed that Virgin Care is seeking to retain the data under its own agreement with NHS Digital. However, at the time of drafting this report, no agreement had been signed by Virgin Care. As a result, a new status of 'Unresolved' has been introduced and raised, since strictly the finding has not been closed, but nor is the ESCCG in a position to close it.	Agreement nonconformity	Unresolved
2.	The ESCCG was unable to identify the Information Asset Owner (IAO) for the data supplied by NHS Digital as required by the DSFC.	Operational Management	The ESCCG has assigned an IAO for the data supplied by NHS Digital and this has been documented. A screenshot of the IAR that included details of the IAO was supplied to the Audit Team.	Agreement nonconformity	Closed

Ref	Finding	Link to Area	Update	Designation	Status
3.	The ESCCG Information Asset Register (IAR) does not include an entry for the data supplied by NHS Digital as required by the DSFC.	Operational Management	The ESCCG has added an entry to the IAR for the data supplied by NHS Digital. A screenshot of the IAR was supplied to the Audit Team. The ESCCG reported the IAR entry is subject to ongoing review.	Agreement nonconformity	Closed
4.	There are no approved data processing agreements in place between ESCCG and the CSU and between ESCCG and Virgin Care to ensure that all parties are aware of their responsibilities and obligations, as required by the DSA.	Operational Management	Since the Audit Team has not seen an approved data processing agreement between the ESCCG and the Commissioning Support Unit (CSU), the finding remains open. An agreement may no longer be required between Virgin Care and ESCCG as there is no contractual agreement between the ESCCG and Virgin Care as it is no longer processing data.	Agreement nonconformity	Open
5.	The ESCCG fair processing notice needs to be reviewed and updated as it does not reflect current practice.	Operational Management	The ESCCG confirmed by email that the fair processing notice has been reviewed to reflect current practice and updated in line with ICO guidelines. A link to the updated privacy notice was provided to the Audit Team.	Agreement nonconformity	Closed
6.	As the Data Controller, the ESCCG has not completed a Privacy Impact Assessment for the data supplied by NHS Digital.	Operational Management	The ESCCG has completed a Data Protection Impact Assessment (DPIA) for the data supplied by NHS Digital. A copy of the approved DPIA was supplied to the Audit Team.	Organisation nonconformity	Closed
7.	The ESCCG Information Governance (IG) Handbook states that both electronic and paper records require classification and that all NHS documents will be classified as Official. The ESCCG was unable to provide evidence that records are being classified in line with its IG handbook.	Operational Management	The ESCCG IG Handbook has been updated and the section on classification has been removed. A copy of the IG Handbook v2.6 was supplied to the Audit Team. However, the Audit Team have noted that NHS England - Document and Records Management Policy recommends protective marking scheme. The ESCCG may wish to reconsider removing the section based on NHS England's guidance.	Organisation nonconformity	Open

Ref	Finding	Link to Area	Update	Designation	Status
8.	The ESCCG has not undertaken a data flow mapping exercise for the data supplied by NHS Digital. The ESCCG IG Handbook and Policy requires a data flow mapping exercise to be completed and reviewed on an annual basis.	Operational Management	The ESCCG has mapped the data flow for the data asset supplied. A high-level data flow map was supplied to the Audit Team.	Organisation nonconformity	Closed
9.	The ESCCG was unable to provide any evidence that staff given additional responsibility for IG had undertaken specialist IG training. The ESCCG IG Policy states that specialist IG training will be provided across the organisation for those staff that are given additional responsibility for IG within their area.	Operational Management	The ESCCG supplied the IAO training material and this was supported by an anonymised staff list and dates when specialist training was undertaken. It was also reported that training is available to all staff on a monthly basis and delivered via an online platform by a member of the Information Governance Team.	Organisation nonconformity	Closed
10.	The ESCCG should consider revising the statement in the DSA “Midlands and Lancashire CSU then pass processed, pseudonymised and linked data to the CCG” as ESCCG confirmed that it does not receive any pseudonymised or linked data from the CSU. ESCCG stated that data supplied by the CSU is aggregated and small numbers supressed.	Operational Management	Subsequent to the statement made during the original audit, the ESCCG has now confirmed that pseudonymised data is received by them for the purpose of redesign and commissioning and planning. The statement in the DSA is correct, and therefore no change is required.	Observation	Closed

Ref	Finding	Link to Area	Update	Designation	Status
11.	The Audit Team suggested that any new DSA and DSFC be reviewed by all stakeholders to ensure that they are aware of their responsibilities and obligations.	Operational Management	The ESCCG confirmed that it plans to share new requirements and documentation associated with the DSA and DSFC with internal teams and also plans to consult with the Senior Information Risk Owner (SIRO), Caldicott Guardian, CSU IG Team and CCG IAOs / Information Asset Administrators and Lay Members. It was also noted that the DSA in the future will be authorised by the SIRO and Caldicott Guardian.	Observation	Open

Table 1: Nonconformities and Observations - ESCCG

Ref	Finding	Link to Area	Update	Designation	Status
12.	A physical control measure with respect to the safeguarding of decommissioned assets was not working correctly.	Access Control	The Audit Team was supplied with a photo which showed that the physical control measure is now working and an explanation on how it works.	Agreement nonconformity	Closed
13.	There was no evidence to show that access to the NHS Digital data is reviewed on a regular basis.	Access Control	The CSU reported that access to NHS Digital data is logged and reviewed, however, no evidence was supplied to support this. The CSU did supply logs on connections made to the network and details supporting this. This was to support reviews undertaken to deactivate unused accounts. No evidence was supplied which showed that individual access to the network folders holding NHS Digital data is reviewed in order that the validity of the list stays current. i.e. if a certain user no longer requires access, they are removed.	Agreement nonconformity	Open

Ref	Finding	Link to Area	Update	Designation	Status
14.	The CSU Password Policy is not consistent with some of the Active Directory Group Domain Controller settings. The CSU stated it had recently undertaken a Cyber Essential assessment and controls had been strengthened as part of this work, however, documentation had yet to be updated to reflect current practice.	Access Control	The CSU Password Policy has been updated. A copy of the Password Policy v2.1 was supplied to the Audit Team. The CSU also supplied a screenshot of the active directory password settings to support the updated policy.	Organisation nonconformity	Closed
15.	One of the CSU SQL processing servers has not been patched / updated since February 2018 due to a migration to a new hosting environment. This timeframe is outside the 30 days stated in the CSU Patching policy and the CSU was unable to supply a risk assessment to support the action. The CSU advised that the patching had been scheduled for July 2018.	Access Control	The CSU supplied evidence to show that the SQL server patching was up to date at the time of the post audit review.	Organisation nonconformity	Closed
16.	During an inspection of a sample of laptops, the Audit Team found the actual Bitlocker encryption level was not as defined by the CSU.	Access Control	The CSU provided evidence that indicated the encryption level has now been correctly configured.	Organisation nonconformity	Closed
17.	The CSU does not have a documented process for the management of IT assets. The CSU IG Handbook procedure simply states that the CSU should establish an approach to monitor the security of the organisation's information assets and physical assets such as IT equipment.	Operational Management	The CSU has developed and implemented an IT Asset Management policy which provides a documented process for the management of IT assets. A copy of the policy v1.1 was supplied to the Audit Team.	Organisation nonconformity	Closed
18.	The CSU should consider adding columns for date, version and review of assessment in the IAR.	Operational Management	The CSU has moved to a new IAR and is looking at developing it further as suggested in the finding.	Observation	Open

Ref	Finding	Link to Area	Update	Designation	Status
19.	The Audit Team suggested the CSU develops and maintains a documented process for the management and review of user accounts including admin/privileged accounts.	Access Control	The CSU has developed and introduced policies and processes for the management and review of user accounts. The Audit Team was supplied with a copy of the User Account Management Policy Network Security Policy.	Observation	Closed
20.	The reconciliation of CSU's IT assets sent to a third-party destruction company is only undertaken at the base unit level. The Audit Team suggested that the serial numbers of the Hard Disk Drives (HDD) are also logged and reconciled to ensure that all assets are accurately accounted for.	Data Destruction	The reconciliation process is now part of the IT Asset Management Policy and a copy of the policy was supplied to the Audit Team. The Audit Team has not seen actual evidence of the reconciliation in practice. However, the CSU was able to supply an asset disposal status report that included details such as HDD serial numbers.	Observation	Open
21.	The CSU has recently migrated to a new storage environment, but no penetration testing of the new environment had been carried out at the time of the audit. The CSU reported that it was in the process of planning and scheduling a test. The Audit Team will need to see the following evidence at the post audit review: • annual penetration test results and associated action plan • application vulnerability test results and associated action plan.	Access Control	A penetration test has been conducted and a summary report and action plan were shared with the Audit Team. There are findings in the action plan that are still open, and the Audit Team require further explanation on the planned action to address them. It should be noted that the CSU did supply an action plan for the actions that remain open, with action dates from 2016/17, even though the penetration test took place after the original audit (July 2018).	Follow up	Open

Table 2: Nonconformities, Observations and Point for follow-up – CSU

Ref	Finding	Link to Area	Update	Designation	Status
22.	NHS Digital undertakes an audit of the data processor services provided by Virgin Care to the CCG in support of the DSA.	Operational Management	In June 2019, the ESCCG terminated its contract with Virgin Care and processing ended around September 2019. At which point the ESCCG asked Virgin Care to delete the data, but Virgin Care declined. The Audit Team has subsequently been informed that Virgin Care is seeking to retain the data under its own agreement with NHS Digital. However, at the time of drafting this report, no agreement had been signed by Virgin Care. As a result, a new status of 'Unresolved' has been raised, since strictly the finding has not been closed, but nor is the ESCCG in a position to close it.	Follow up	Unresolved

Table 3: Point for follow-up - Virgin Care