Directorate	**Assurance and Risk Management**	Project	**Data Sharing Audits**
		Status	**Final**
Director	**James Hawkins**	Version	**1.0**
Owner	**James Hawkins**	Version issue date	**11/03/2021**

NHS Digital Post Audit Review of Data Sharing Activities: Ernst & Young LLP

1 Audit Summary

1.1 Purpose

This report provides the formal closure of the data sharing audit of Ernst and Young LLP (EY) on 5 and 6 June 2018 against the requirements of the data sharing framework contract (DSFC) CON-344745-W9L4X and the data sharing agreement (DSA) NIC-369596-F69V v3.8 with respect to the provision of:

Dataset	Classification of Data	Dataset period
Secondary Uses Service Payment by Results Episodes	Anonymised/Pseudonymised, Non-sensitive	2014-15 to 2017-18
Secondary Uses Service Payment by Results Spells	Anonymised/Pseudonymised, Non-sensitive	2014-15 to 2017-18
Secondary Uses Service Payment by Results Outpatients	Anonymised/Pseudonymised, Non-sensitive	2014-15 to 2017-18
Secondary Uses Service Payment by Results Accident and Emergency	Anonymised/Pseudonymised, Non-sensitive	2014-15 to 2017-18

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 involved an assessment of the action plan and supporting evidence supplied by EY between January 2019 and August 2020. It involved a desk-based review and a video conferencing session in January 2020. The video conferencing session allowed evidence held to be interactively viewed. Additional supporting evidence was supplied via email following the session. Supporting evidence was also supplied by the Data Access Request Service in December 2020.

Based on this post audit review the nonconformities have been closed. There are 3 observations which are still open, however, no further follow-up is planned by the Audit Team. An observation is a situation where a requirement is not being breached but a possible improvement or deficiency has been identified by the Audit Team.

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

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

1.5 Data Recipient's Action Plan

As NHS Digital has closed all of the nonconformities, no further action is required by the Audit Team. There are three observations which are still open, and EY should follow up until the actions against the findings are completed.

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

Table 1 identifies the 1 agreement nonconformity, 2 organisation nonconformities and 11 observations raised as part of the original audit.

Ref	Finding	Link to Area	Update	Designation	Status
1	EY stated it does not backup the NHS Digital provided data held within the third-party data centre. The DSFC requires data is backed up on a regular basis. EY participated in discussions with NHS Digital in terms of the remit of its contract with the third-party supplier, however, EY did not discuss with NHS Digital the lack of backups and that it had taken this decision as an operational risk.	Information Transfer	EY stated that data provided by NHS Digital has been transferred to a new cloud storage environment. The Data Access Request Service (DARS) has informed the Audit Team that they have approved the cloud storage environment.	Agreement nonconformity	Closed
2	The EY Global Information Security Password Policy does not distinguish and highlight the difference between the corporate and guest Wi-Fi access. During the audit the Audit Team found the guest Wi-Fi access at EY's Leeds office had a password length of less characters than specified in the password policy	Access Control	EY provided an extract from its Password Policy which was updated in April 2019. The applicability section has been amended to clarify that the policy only covers corporate access to EY IT infrastructures. EY also stated that there is no separate policy for guest Wi-Fi access.	Organisation nonconformity	Closed
3	Although EY stated a Privacy Impact Assessment (PIA) had been completed for the Secondary Uses Service (SUS) dataset, the PIA document provided to the Audit Team refers to Hospital Episodes Statistics (HES) data. EY no longer receive any HES data from NHS Digital and has not received or processed any HES data since approximately 2014. From email evidence the Audit Team's view was that the name had been incorrectly recorded.	Risk Management	EY provided a copy of a PIA completed in June 2019. The updated PIA covered the processing of SUS data rather than HES data. In addition, the PIA also included migration to the new cloud storage environment.	Organisation nonconformity	Closed

Ref	Finding	Link to Area	Update	Designation	Status
4	The Audit Team suggested that an internal audit / compliance assessment be undertaken within health analytics by EY, with specific reference to data supplied by NHS Digital. No such audit/assessment had been undertaken to date nor is one currently scheduled.	Operational Management	EY stated that an internal assessment has not yet taken place but expect to undertake a review and assessment in due course.	Observation	Open, but not for follow-up
5	The Audit Team suggested that EY clarifies the review period for its policies and procedures. Verbally it was suggested by EY that the review period was annual, though not all the policies and procedures had been reviewed or updated within the past year.	Operational Management	EY provided a copy of its Global Information Security Policy which has been updated to reflect the requirement for annual updates of all Information Security and supporting policies. EY stated that the review periods for the other policies varies from policy to policy.	Observation	Open, but not for follow-up
6	There is no documented process for the management and control of local administration / privileged accounts for the third-party data centre environment.	Access Control	Prior to the migration to the cloud storage environment, EY provided a copy of a flow chart to show the controls in place for privileged / administration accounts for the data centre. EY are currently in the process of reviewing its DSA and DSFC and is proposing the destruction of data currently held and termination of its contract. If at anytime in the future EY receives any new data, it will review and renew its access policies.	Observation	Closed
7	EY established a Health Data Panel (HDP) in 2016 to formally review all data processing requests. The Audit Team suggested that the current version of the Terms of Reference for the HDP be updated to take into consideration the following points: • the document management page has not been completed; and • the frequency of meetings has changed from monthly to weekly.	Operational Management	EY provided a copy of its updated Terms of Reference for the HDP, which included the following changes: • the document management page had been completed and updated • the frequency of meetings had been changed to fortnightly.	Observation	Closed

Ref	Finding	Link to Area	Update	Designation	Status
8	Two of the superusers of the SUS data had not completed their annual Super-User SUS Technical Training Refresh. EY advised the Audit Team that one of the users is on long term secondment and the other user had not accessed the SUS environment for over 12 months. The Audit Team suggested that EY clarifies the status of these users and determine whether they need to remain as superusers and schedule their refresher training or disable their accounts to SUS.	Operational Management	EY provided evidence that the two superusers access rights to the SUS environment had been removed.	Observation	Closed
9	The Audit Team suggested that a date field be added to the Privacy Impact assessment (PIA) template or Data Protection Impact Assessment (DPIA) equivalent. This addition will ensure that there is an adequate approval and audit trail	Operational Management	EY provided a copy of the PIA questionnaire completed for data provided by NHS Digital. The template now has a date field. Furthermore, EY stated that its global PIA tool automatically records the date when a PIA is first submitted for review and a date for when the final PIA is sent out to the global network.	Observation	Closed
10	The Audit Team suggested EY determines whether the risk rating using their Information Security Policy (classification of electronic information) (C1 to C4) should be directly comparable with risk rating identified within their Information Security Policy (Code of Connection) (Low/Moderate/High).	Risk Management	EY does not have a document that directly illustrates the mapping between the Security Risk Profile rating (low, mod, high) with the Information Classification Policy classification levels (C1, C2, C3, C4). However, the updated Security Risk Profile questionnaire, does link the classification levels to the Security Risk Profile rating.	Observation	Closed
11	The Audit Team suggested EY develop and implement a process for the management of administration / local user accounts for staff moving within EY to ensure that this is appropriately controlled and recorded.	Operational Management	The EY Health Data Governance panel reviews changes to access rights to ensure access is restricted to the appropriate personnel including movers. To further support this, EY provided a copy of the minutes from a meeting held in March 2018 which confirms that the list of superusers are reviewed and monitored.	Observation	Closed

Ref	Finding	Link to Area	Update	Designation	Status
12	EY as part of its vendor assessment process with respect to vendors who have multiple global sites should consider conducting assessments at alternative locations rather than focussing on one location.	Risk Management	EY declared that it has begun the first phase of implementation of its monitoring program, which includes site visits and virtual monitoring of suppliers that have multiple sites. For example, EY is about to conduct a site visit to a support site managed by a global vendor.	Observation	Open, but not for follow-up
13	Although EY provided some examples of specialist training undertaken by the Information Asset Owner (IAO) which includes mandatory training for General Data Protection Regulations (GDPR) the Audit Team suggested that consideration should also been given to the specialist IAO training currently available on the Department of Health Data Security and Protection Toolkit.	Operational Management	EY provided evidence that the IAO had attended and participated in regular mandatory training which includes GDPR.	Observation	Closed
14	The Audit Team suggests that version control is applied to a completed Security Risk Profile to ensure that there is a full audit trail and is trackable.	Risk Management	The Security Risk Profile excel document is no longer used as the main document. Information is now entered into a new application “eGRC” which maintains a change history. EY provided a screenshot of a completed action from this application. The screenshot included full details of description, status and start/due date.	Observation	Closed

Table 1: Nonconformities and Observations