Directorate / Programme	**Assurance and Risk**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Carl Vincent**	Version	**1.0**
Owner	**Rob Shaw**	Version issue date	**03/08/2018**

NHS Digital Audit of Data Sharing Activities: Device Access UK Ltd

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at Device Access UK Ltd (referred to as DAUK) on 19 and 20 June 2018. It provides an evaluation of how DAUK conforms to the requirements of the data sharing framework contract (DSFC) CON-321172-W8X4S and the data sharing agreement (DSA) NIC-05429-H7X6R-v3.2 with respect to the provision of:

Dataset	Classification of Data	Dataset period
Hospital Episode Statistics (HES) – Admitted Patient Care	Anonymised/Pseudonymised, Non-sensitive	2012/13 – 2018/19
HES – Critical Care	Anonymised/Pseudonymised, Non-sensitive	2012/13 – 2018/19
HES – Outpatients	Anonymised/Pseudonymised, Non-sensitive	2012/13 – 2018/19
HES – Accident and Emergency	Anonymised/Pseudonymised, Non-sensitive	2012/13 – 2018/19

The Data Controller is DAUK.

The report also considers whether DAUK 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 Audit Type and Scope

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

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 Data Recipient's Acceptance Statement

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

1.5 Data Recipient's Action Plan

DAUK 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 DAUK to confirm the findings have been satisfactorily addressed.

2 Findings

Table 1 identifies the 7 agreement nonconformities, 3 organisation nonconformities and 10 observations raised as part of the audit.

Ref	Finding	Link to Area	Clause	Designation	Notes
1.	A significant number of management policies and procedures are not fit for purpose and need to be reviewed and updated. The controls defined in the documents are not reflected in current practice. There are also changes to current practices which are not defined in the documents.	Operational Management	DSFC, Schedule 2, Section A, Clause 3	Agreement nonconformity	
2.	The Audit Team identified two contractors that have access to the NHS Digital data who had not completed the IG training in the last 12 months. The DSFC requires all users with access to NHS Digital data to complete suitable training on an annual basis.	Operational Management	DFSC, Schedule 2, Section A, Clause 1.2.2	Agreement nonconformity	
3.	The Secure Electronic File Transfer (SEFT) username and password supplied by NHS Digital is being shared with a contractor. SEFT details are supplied on the understanding that they are known only by a named individual. Similarly, a common login account with enhanced privileges is used on a standalone PC which is used to process and store NHS Digital data.	Access Control	DFSC, Schedule 2, Section B, Clause 4.6 NHS Digital, SEFT email sent to DAUK	Agreement nonconformity	
4.	The USB portable device which is used to transfer HES data downloaded from the NHS Digital SEFT portal to the standalone PC is not encrypted.	Access Control	DFSC, Schedule 2, Section A, Clause 4.7	Agreement nonconformity	
5.	The IT assets used by DAUK to access, process and store NHS Digital data were not included on an equipment asset register. In addressing this finding, DAUK should consider adding the serial numbers of the Hard Disc Drives (HDD) to the register as this will allow reconciliation between equipment sent for destruction and a third-party contractor's data destruction certificate in order to account for all devices.	Access Control	DFSC, Schedule 2, Section A, Clause 4.7	Agreement nonconformity	
6.	The laptop used to manage the download of NHS Digital data from the SEFT portal was encrypted overnight during the audit. It was identified that the encryption process had failed and the laptop would not boot. The Audit Team was therefore unable to carry out checks on the laptop.	Access Control	DFSC, Schedule 2, Section A, Clause 4.4	Agreement nonconformity	

Ref	Finding	Link to Area	Clause	Designation	Notes
7.	The password policy is not system enforced on the standalone PC used to process and store NHS Digital data.	Access Control	DFSC, Schedule 2, Section A, Clause 4.2	Agreement nonconformity	
8.	The standalone PC used to process and store the data does not lockout after a period of inactivity. The company's Access Control Procedure states that the password locked screen saver is enabled after 15 minutes of inactivity.	Access Control	Access Control Procedure Clause 5.4.5 and 5.4.6	Organisation nonconformity	
9.	DAUK has developed an internal audit plan for 2016 and 2017 which listed 12 audits, however, only 1 audit had been completed.	Operational Management	DAUK, 2016 and 2017 Audit Plan	Organisation nonconformity	
10.	A number of checks have not been completed against DAUK own procedures, including new starter checklist, user access agreements and policies and procedures acceptance sign off etc.	Operational Management	DAUK, New starter checklist DAUK, User access agreement DAUK, Policies and procedures acceptance sign off	Organisation nonconformity	
11.	In its recent guidance, the Information Commissioner's Office (ICO) states "information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR". As a result, DAUK should consider conducting a Data Protection Impact Assessment (DPIA) for the supplied data.	Operational Management	ICO's Guide to the General Data Protection Regulation (GDPR)	Observation	
12.	DAUK should consider running a security baseline assessment tool to assess the security controls enforced on the machine used to process and store NHS Digital data.	Access Control		Observation	
13.	DAUK should undertake a compliance check against both the DSFC and DSA. This check should also be carried out prior to signing a new DSFC and DSA to ensure the DAUK is compliant with any new requirements.	Operational Management		Observation	
14.	DAUK should consider carrying out a risk assessment at the current processing and storage location to assess the physical access controls. This may also highlight the need to enhance some of the controls. A further assessment should be considered against the options being considered on potential new processing and storage locations. Any changes to the processing and storage locations will require advance notification to NHS Digital.	Risk Management		Observation	

Ref	Finding	Link to Area	Clause	Designation	Notes
15.	DAUK should determine how to securely store copies of the encryption keys for the standalone PC used to process and store NHS Digital data.	Access Control		Observation	
16.	The data asset register should be expanded to include columns for links to data destruction certificates, date of data destruction, expiry date for DSFC and DSAs etc.	Operational Management		Observation	
17.	DAUK should consider developing a procedure that covers hardware and data destruction.	Data Destruction		Observation	
18.	DAUK should consider developing a control spreadsheet to manage the contractual status of external contractors, Non-Disclosure Agreements, training records etc.	Operational Management		Observation	
19.	DAUK should assess and compare the data destruction software being used against the NHS Digital guidance to check for compliance. DAUK should consider enabling the logs on the software to provide an audit trail.	Data Destruction		Observation	
20.	DAUK should consider updating the network topology diagram to reflect current practice.	Information Transfer		Observation	

Table 1: Nonconformities and Observations

2.1 Supplementary Notes

No notes.

2.2 Use of Data

DAUK 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

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

Organisation	Territory of Use
DAUK	England / Wales

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
DAUK	Backup external disk	DSA retention period

Table 3: Data Retention Period

2.5 Good Practice

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

- DAUK was able to demonstrate the direct benefits to health and social care from the use of NHS Digital data.

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.