Directorate / Programme	**Care Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Catherine O'Keeffe**	Version	**1.0**
Owner	**Sean Walsh**	Version issue date	**13/10/2017**

NHS Digital Audit of Data Sharing Activities: Pathway Communications

1 Audit Summary

1.1 Purpose

This document records the key findings of a data sharing audit at Pathway Communications on the 15 and 16 August 2017. It provides an evaluation of how Pathway Communications conforms to the requirements of the Data Sharing Framework Contract (DSFC) CON-361439-K1N1H (which expired at the end of July) and the data sharing agreement (DSA) DARS-NIC-391618-M3X6R with respect to the provision of HES Outpatients and Admitted Patient Care data. The report also considers whether Pathway Communications conforms to its own policies and procedures.

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

1.2 Scope and Assurance Statement

The audit considered the fitness for purpose of the main processes with respect to data handling at Pathway Communications along with its associated documentation against the scope areas shown in Table 1.

The NHS Digital Audit Team has assigned the following assurance ratings to these areas based upon the findings of the audit.

Information Transfer	Limited assurance
Access Control	Unsatisfactory assurance
Data Use and Benefits	Substantial assurance
Risk Management	Moderate assurance
Operational Management and Control	Limited assurance
Data Destruction	Moderate assurance

Table 1: Scope and Assurance rating

Detailed findings related to the areas of scope are detailed in Table 2.

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, there is high 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 Pathway Communications under the terms and conditions of the data sharing agreements signed by both parties.

1.4 Response

Pathway Communications has reviewed this report and confirmed that it is accurate.

As Pathway Communications has elected not to renew its DSA then no action plan will be requested and no post audit review will be conducted. Should Pathways decide to submit a data sharing application in the future then the findings presented in this report will be followed up as part of the new application.

2 Findings

Table 2 identifies the 2 major nonconformities, 3 minor nonconformities and 11 observations raised as part of the audit.

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

Ref	Comments	Link to Area	Clause	Designation	Notes
1.	The server and laptops are not password protected / locked after a period of inactivity. The company's Acceptable Use Policy states "Computing devices must automatically be logged off/locked or protected with a screen locking mechanism if left idle for more than 5 minutes".	Access Control	Pathway, Acceptable Use Policy, 1.4	Major	
2.	Data is being stored and processed at a location not declared on the DSA. *The new location was notified to the Audit Team as part of the audit preparation stage and formally updated with NHS Digital through the Data Access Request Service online portal on 18 August 2017.*	Information Transfer	DSA, Annex A, 2a and 2b	Major	
3.	The Password Policy is not system enforced though local group policies on the individual laptops although it was reported that the policy was being adhered to manually. Account lockout is also not currently configured on machines. *Local group policies on the laptops were changed overnight to align with the Password Policy.*	Access Control	Pathway, Password Policy, 20.2	Minor	
4.	The hard discs and the USB portable device (which is used to transfer HES data between a laptop, used solely at present for downloading the data files from the NHS Digital SEFT portal, to an isolated server) are encrypted to AES 128. The company's Password Policy defines encryption to AES 256. *The encryption setting on the laptops was changed to AES 256 overnight. Other devices are still to be changed.*	Access Control	Pathway, Password Policy, 20.3	Minor	
5.	The designated users involved in processing the data have not undertaken appropriate training in accordance with the DSFC. The company is planning to send staff on such training and the Audit Team provided links to the NHS Digital Information Governance Toolkit resources.	Operational Management	DFSC, Schedule 2, Section A, 1.3.2	Minor	

Ref	Comments	Link to Area	Clause	Designation	Notes
6.	As the main server used to hold and process the data is isolated from the local network and the Internet, it does not receive regular patches nor is any anti-virus installed. This is not explicit in the Mobile and Computing Devices Policy which states that any company computer shall be kept up-to-date and protected by an anti-virus program. The policy needs to reflect this situation given the isolated nature of the server and record that it will be periodically patched by the IT provider.	Operational Management	Pathway, Mobile and Computing Devices Policy, 16.3	Observation	
7.	The HES data should be classified according to the company's information classification scheme.	Operational Management	Pathway, Information Handling Policy, 15.3	Observation	
8.	The policies and procedures need careful reviewing to ensure current practices are correctly described.	Operational Management		Observation	
9.	The risk assessment needs to be reviewed and extended as necessary to ensure that appropriate risks and mitigation controls are captured. This may also highlight the need to enhance some of the physical security controls.	Risk Management	DSFC, Schedule 2, Section A, 4.9	Observation	
10.	The IT provider needs to regularly review the configuration of the firewall to ensure any new firmware is applied and the rules checked for validity and appropriateness. The company has subscribed to an annual update subscription service for the firewall.	Access Control		Observation	
11.	The IT providers should be given sight of the DSFC and DSA to ensure that the technical requirements are being properly adhered to. This also conforms to the system and service reviews which are defined in the Outsourcing Policy. The Audit Team suggested that as part of such reviews the IT providers could run tools, such as Microsoft Baseline Security Analyser, to ensure the appropriate configuration of the system.	Operational Management	Pathway, Outsourcing Policy, 19	Observation	
12.	The incident reporting procedure should be updated to include the timely reporting of any incidents to NHS Digital. The procedure should also include reference to NHS Digital guidance on incident reporting.	Operational Management	DSFC, Part 2, 4.3.6	Observation	
13.	The company needs to ensure that it only retains the last 36 months of data in accordance with the DSA as future periods are downloaded.	Operational Management	DSA, Annex A, 8a	Observation	

Ref	Comments	Link to Area	Clause	Designation	Notes
14.	The company needs to ensure the source of the data is mentioned in any future publications that are prepared using NHS Digital's data.	Operational Management		Observation	
15.	The process checklist used to define the download and handling of HES data needs to be reviewed to ensure that the downloaded dataset is correctly stored in the encrypted portion of the USB memory stick.	Access Control	Pathway, Handling HES data checklist	Observation	
16.	The company needs to establish with the IT provider that the data erasing application is appropriate for portable solid state devices and it conforms with latest NHS Digital guidance. *The Audit Team provided a copy of the guidance during the audit.*	Data Destruction		Observation	

Table 2: Nonconformities and Observations

2.1 Supplementary Notes

Not applicable.

2.2 Data Location

Pathway Communications confirmed that processing and storage, including disaster recovery and backups, of the data was limited to the location shown in Table 3.

Data Location	England

Table 3: Data Location

2.3 Backup Retention

No backups are currently being taken.

2.4 Good Practice

In addition to the findings presented in Table 2 the Audit Team noted the following areas of good practice:

- The results of the analysis being undertaken on the data are of benefit to health and social care through the optimisation of clinical pathways.

2.5 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.