|  |  |  |  |
|---|---|---|---|
| Project / Programme | **Data Dissemination Services** | Project | **Data Sharing Audits** |
|  |  | Status | **Approved** |
| Director | **Terry Hill** | Version | **1.0** |
| Owner | **Rob Shaw** | Version issue date | **19/04/2017** |

# NHS Digital Technical Audit of Data Sharing Activities: Harvey Walsh Limited

# Contents

# Executive Summary

This document records the key findings of a technical audit of Harvey Walsh Limited (Harvey Walsh) following a joint meeting between NHS Digital and Harvey Walsh in September 2016 that concluded the company had breached its Data Sharing Agreement by using an undeclared third party to hold NHS Digital data used by its online system known as AXON.

Following identification of this breach by NHS Digital, Harvey Walsh took the voluntarily decision to take the AXON system offline. The hardware used to hold the application and data was purchased from the third party and transferred to a secure location under the control of Harvey Walsh.

The purpose of this technical audit was to examine the data transfer and storage of the AXON system, access control, small numbers suppression and the use of data. However, as the organisation had not been previously audited by NHS Digital the Audit Team extended the scope to include other areas normally examined as part of a data sharing audit.

Due to the nature of the audit, the process by which it was conducted and recorded differs from the published routine data sharing audits conducted by NHS Digital. Specifically, this audit was conducted over an extended time frame which allowed Harvey Walsh to address the shortcomings identified by the Audit Team and the Data Access Release Service (DARS) Team. As a result, conclusions are presented as statements rather than as nonconformities or observations based on the evidence presented by Harvey Walsh.

From the on-site visits and the evidence reviewed, further changes had to be made by Harvey Walsh to address shortcomings identified. Notably, this has resulted in assurances being provided on the transfer of the AXON system to a Harvey Walsh secure location, a redesign of the AXON model to meet NHS Digital requirements and an independent third party security assessment on the AXON web application.

Harvey Walsh was given permission by NHS Digital to bring the AXON system back online on the 8 February 2017, when a new Data Sharing Agreement was signed after issues identified in this audit and by the DARS team had been addressed.

The Audit Team has concluded from this extended review that the operational management and controls that have been established are reasonable and have addressed the cause of the identified breach.

In summary, it is the Audit Team's opinion that based on evidence presented during the audit there is low risk of inappropriate exposure and / or access to data provided to Harvey Walsh by NHS Digital.

# 1 About this Document

## 1.1 Introduction

The Review of Data Releases by the NHS Information Centre produced by NHS Digital Non-Executive Director Sir Nick Partridge recommended that NHS Digital should implement a robust audit function that will enable ongoing scrutiny of how data is being used, stored and deleted by those receiving it.

In August 2014, NHS Digital commenced a programme of external audits with organisations with which it holds data sharing agreements.

## 1.2 Background

Harvey Walsh uses pseudonymised, monthly refreshed Hospital Episode Statistics (HES) data to undertake analysis, develop services and provide solutions to support commissioning for NHS organisations. This support includes access to an online system known as AXON where data is presented in different views. Harvey Walsh also utilises HES data to provide services to commercial organisations within the pharmaceutical, medical device industry and patient organisations. These organisations use the outputs and insights to work collaboratively with NHS organisations to promote health and improve the wellbeing of patients.

In September 2016, Harvey Walsh was found to have breached its Data Sharing Agreement by using a third party to host the storage of NHS Digital data used for the AXON system. This third party had not been declared within the Data Sharing Agreement. Additionally, NHS Digital found that the AXON system backend database held record level data that was not aggregated or small numbers suppressed. The AXON front end was aggregated and small numbers were suppressed, however no secondary suppression was being applied.

As a result of this breach, Harvey Walsh took the voluntarily decision to take the AXON system offline. Harvey Walsh then purchased and transferred the hardware holding NHS Digital data and application from the third party to a secure location under its control.

## 1.3 Purpose

This report provides an evaluation of how Harvey Walsh has adapted its processes in order to conform to the requirements of its Data Sharing Framework Contract and a Data Sharing Agreement. This report provides a summary of the key findings.

## 1.4 Presentation of Findings

As this technical audit involved a more detailed and protracted review, this report does not use the established approach taken to the reporting of data sharing audit findings (i.e. nonconformities and observations).  Sections 2 and 3 do, however, present findings both from the on-site visits and at the time of writing in order to present a balanced view.

## 1.5 Audience

This document has been written for the NHS Digital Director of Data Dissemination Services. The report will be published in a public forum.

## 1.6 Scope

The audit considered the fitness for purpose of the main processes of data handling at Harvey Walsh along with its associated documentation.

The audit sought to elicit for Data Sharing Agreement (DSA) NIC-05934-M7V9K whether:

- the organisation was adhering to the requirements of the  data sharing framework contract and the data sharing agreement;
- the data handling activities within the organisation pose an unacceptable risk to confidentiality or to NHS Digital; and
- the organisation conforms to its own policies and procedures.

As part of the audit, the Audit Team examined the AXON system and specifically the data transfer and storage of the AXON system, access control (specifically registration, deregistration and password control), small numbers suppression and the use of data.

## 1.7 Audit Team

The Audit Team was comprised of senior, certified and experienced NHS Digital personnel. Qualifications held by the Audit Team include Lead Auditor/Auditor ISO 9001:2008 (Quality management systems), Lead Auditor ISO 27001:2013 (Information security management systems), Certificate Information System Auditor (CISA) and Masters in Information Rights Law and Information Governance.

## 1.8 Response

Harvey Walsh has reviewed this report and confirmed that it is accurate.

# 2 Audit Findings

This section presents the key findings arising from the audit, which included:

- an on-site visit to Harvey Walsh's offices in Runcorn on 13, 14 and 26 October 2016; and
- a review of evidence over the period from October 2016 to March 2017.

## 2.1 Information Transfer

The raw NHS Digital data is downloaded from NHS Digital via Secure Electronic File Transfer (SEFT) and saved onto an in-house server within Harvey Walsh site. The data is processed and made available for bespoke analysis and the AXON system.

For the bespoke analysis, an extract of the processed data is transferred and saved onto four desktop PCs. Each PC has two encrypted Solid State Drives (SSD) and a Hard Disk Drive (HDD). The data is processed on these local machines by the SQL Analyst team. Only certain employees have access to the record level data and each machine is within a locked office.

The Audit Team noted that the DSA did not include full details of all the servers and the four PCs that hold NHS Digital data. The Audit Team also noted that there were high level information flow charts available on the handling of NHS Digital data however these could be improved with supporting procedures.  Both the findings have been addressed.

## 2.2 Access Control

The Head of IT is responsible for the overall network and maintaining IT equipment, including the provision of access onto the network.

Management authorisation is required for new starters to gain access to the network. Access to the folder where NHS Digital data resides requires senior management approval. Removal of access is managed by the Head of IT.

The Access Control policy and procedure covers the process for user access management, password management, review of access rights, user responsibilities and network access control.

The Audit Team carried out checks during the onsite visit and identified some IT security control weaknesses on the internal network. These weaknesses included issues with the password policy, the level of encryption on the SSDs of the four PCs, an unsupported server operating system (and SQL server) and an internal network switch that had reached end of support.  The risk with the network switch was low however Harvey Walsh were only made aware of this risk when identified by the Audit Team.

It was also found that user access rights were reviewed at the internal Information security meeting, however the user access listed on the review document and the users with accounts on the servers did not reconcile.

All the issues identified were on the internal network and they have been addressed at the time of drafting this report.

Following the on-site visit the Audit Team highlighted that there was a minimal risk of software caching data onto the local hard drive of the PC's, Harvey Walsh encrypted the hard drives to mitigate any such risk.

NHS Digital data on Harvey Walsh servers is backed up to a Network Attached Storage (NAS). The Audit Team found that the NAS was not encrypted during the initial audit visit. This data is now software encrypted to 256bit AES.

Access to the computer room where the servers and backup system holding NHS Digital data is housed is restricted to key staff. The computer room has a number of physical controls.

An external third party has conducted an external infrastructure security assessment of specific internet facing hosts in order to identify security issues Harvey Walsh network. The assessment was commissioned after senior management carried out an internal risk assessment. The assessment was carried out on the 14 November followed by a retest on the 23 November 2016.

## 2.3 Data Destruction

During the discussions it was highlighted that a logical delete would be used to delete NHS Digital data on the server. The Audit Team recommended during the initial visit that Harvey Walsh carry out a risk assessment on the use of third party data deletion software to ensure data is permanently deleted in line with NHS Digital guidance.

Harvey Walsh has received a request from NHS Digital to permanently delete some of the data and following the initial onsite audit meeting, Harvey Walsh have discussed and agreed the methodology for destruction with the DARS team.

As a result, the agreed data has been destroyed on the servers using a third party data deletion system, encrypted CDs have been shredded and the backup hard drives have been degaussed. This has been completed in conjunction with discussions with the DARS team and certificates supporting the destruction have been forwarded as documented assurance.

## 2.4 Operational Management and Control

Harvey Walsh has been certified to ISO 27001:2013 since 2010.

Staff members are required to sign a confidentiality agreement and individual user agreement prior to accessing any record level data. The Audit Team reviewed examples of completed forms.

Harvey Walsh commission's a third party to undertake internal audit functions for physical security, the annual submission of the Information Governance Toolkit (IGT), annual information governance risk assessment and documentation review. This is managed within quarterly Information Security meetings and is reviewed annually at the Management Review meeting.

Information governance and information security related policies are also reviewed within the above framework. It was noted that the Incident Reporting procedure did not include the Serious Incident Requiring Investigation (SIRI) timescales. These timescales were added following the on-site visit.

Furthermore, the Information Classification and Exchange procedure did not reflect current practice for example in relation to where confidential data is stored and access is based upon job role not by grade as specified in the document. This issue has been addressed.

Harvey Walsh has updated its Information Commissioners Office's Data Protection Registration to include 'data is processed about health care users and will be shared with/accessed by health care suppliers/professionals' following discussions with the Audit Team.

Contract services and project profiles are created on Harvey Walsh's contract management system, work is allocated to the data analyst team through a work management system and a quality assurance process is established for sign off of data analysis. However, whilst the Chief Information Security Officer (CISO) completes checks before signing off all final research papers before forwarding to the customer, this element of the process is not documented. This issue has been addressed.

Whilst it is recognised that impact on privacy is considered in the development state of a project this is not formally recorded and could be included in Standard Operating Procedures (SOP) for handling HES data. Following the on-site visit Harvey Walsh produced SOPs for handling of data. Privacy Impact Assessment (PIA) was also included within the JIRA work management system.

The IT asset register had a high-level summary of assets held by Harvey Walsh, however not to the level of detail to allow an audit trail on specific assets holding NHS Digital data. This was addressed after the onsite audit.

The Information Asset Register (IAR) did not display the Information Asset Owner (IAO) but instead showed the person as the Information Asset Administrator (IAA). The IAR is reviewed annually within the Management Review meeting. The IAR was updated following the on-site visit to include the correct IAO and IAA.

At the time of the on-site visit no specialist training for the IAO and the IAA had been undertaken. In December 2016, the IAO and support staff undertook specialist Data Protection Act training through an external provider and the learning was cascade to the team.

A change control form is created for any system changes and completed forms are held and monitored in a manual filing system. The Audit Team recommended that a log of change control forms be kept and this was implemented following the on-site visit.

A third party conducts an annual corporate risk assessment. A risk assessment report is provided to the Management Review meeting and reviewed. Any emerging corporate risks are discussed immediately and then added to the risk register, if required. Risks in the risk register are reviewed on a regularly basis by management in line with good practice.

## 2.5 Use and Benefits of Data

The Audit Team viewed examples of research papers and examples of data analyses provided to customers in addition to that supplied by the access to the AXON system. No evidence of data linkage of HES data and other sources of data was found.

Any analysis provided to third parties is in aggregate format only, with small numbers suppressed in line with the HES Analysis guide. A front sheet is included detailing the project and purposes for which HES can be used.

## 2.6 AXON Online System

Harvey Walsh use pseudonymised, monthly refreshed HES data to undertake analysis, develop services and provide solutions to support commissioning for NHS organisations. This includes access to an online system called AXON, where data is presented in different views. Access to the system is through a username and password. The system is managed by Harvey Walsh.

It was identified during the process of submitting a renewal to its existing agreement in September 2016 that a third party hosted the AXON system that included NHS Digital data on its IT hardware on behalf of Harvey Walsh, which was not detailed in the DSA. This was a breach of the DSA.

During this process, it was also identified that the AXON system backend database held record level data that was not aggregated or small numbers suppressed. The AXON front end was aggregated and small numbers are suppressed, however no secondary suppression was being applied.

### Third party host

Immediate action was taken by Harvey Walsh following the identification of the breach. An email was sent by Harvey Walsh to all AXON customers to notify them that the system would be offline and an explanation provided on the background. Furthermore, Harvey Walsh purchased and transferred the hardware holding NHS Digital data from the third party to its own location.

The Audit Team was informed that the data on the backup server held by the third party has been destroyed and data destruction certificates provided to NHS Digital. The backup is now managed by Harvey Walsh and stored at its own premises.

An email was provided from the third party hosting company that old hard drives used to hold Harvey Walsh data (including NHS Digital data) had been decommissioned to HMG Infosec Standard 5 (IS5). There were no data destruction certificates available to support the hard disk destruction as Harvey Walsh had not requested the certificates at the time of when the hardware was decommissioned.

The AXON system had been offline from the 5 September 2016 following identification of the above breach by NHS Digital. The audit trail reports shown to the Audit Team during the onsite visit supported that the AXON system has been offline since that date and no customer has been able to access the system.

Harvey Walsh was given permission by NHS Digital to bring the AXON system back online on the 8 February 2017, when a new DSA was signed after issues identified in this audit and by the DARS team had been satisfactorily addressed.

### AXON model

Harvey Walsh have developed and built a new a model for the AXON backend database in discussion with the DARS team. The model includes data that is aggregated with the appropriate small number suppression. The solution has been built and tested by Harvey Walsh. The DARS team has signed off the AXON model that it meets NHS Digital requirements.

### Registration and deregistration process

At the time of the onsite visit, there was a process in place to register and deregister accounts on the AXON system; however the process was not documented.

Any user that requires access to the AXON system has to be nominated to the AXON Lead by the customer. The user is validated by Harvey Walsh and an account is setup on the AXON system. The user needs to complete training prior to receiving login details.

AXON users are requested to change the password manually on a regular basis. Following the onsite audit, Harvey Walsh has improved this control by implementing a system enforced password change. Users are now prompted to change the password every 90 days. Harvey Walsh has provided the source code to support this change.

AXON customers are provided with a usage report including user statistics on a monthly basis. It is the customer’s responsibility to review the list of users and let Harvey Walsh know of any leavers and users no longer requiring access.

### Security assessment

A web application security assessment was carried out on the AXON application using dummy data on the 19 January 2017, followed by two retests on the 31 January and 1 February 2017 by an independent third party.

# 3 Conclusions

This section presents the key findings of this audit based on the:

- findings from the on-site visits; and
- revised findings based upon subsequent discussions and review of evidence.

The main findings are:

### Information transfer

- The DARS application form now includes full details of the key servers and the four PCs that hold NHS Digital data.
- New procedures have been included with the information flow charts to support the handling of NHS Digital data.

### Access control

- The internal network issues identified have been addressed. This includes updating the password policy on machines, increasing the level of encryption on the SSDs, updating the server operating system (and SQL server) to a supported version and replacing the internal network switch to one which is supported by the manufacturer.
- The user access right list has been updated and now reconciles with the list of users with accounts on the servers.
- An external third party has conducted an external infrastructure security assessment of specific internet facing hosts in order to identify security issues with the Harvey Walsh network. The assessment was carried out on the 14 November followed by a retest on the 23 November 2016.

### Data destruction

- Harvey Walsh received a request from NHS Digital to permanently destroy some of the NHS Digital data it held. The data has been destroyed on the servers using specialist data deletion software, encrypted CDs have been shredded and the backup hard drives have been degaussed.

### Operational planning and control

- The Incident Reporting procedure has been updated to include the Serious Incident Requiring Investigation (SIRI) timescales.
- The Information Classification and Exchange procedure has been updated to reflect current practice.
- The CISO completes checks before signing off all final research papers before forwarding to the customer. This process is now documented.
- Privacy impact was considered before but is now formally recorded in the Standard Operating Procedures (SOP) for handling HES data.

- The IT asset register now includes further details that allow an audit trail on specific assets holding NHS Digital data.
- The IAR has been updated to include the correct IAO and IAA.
- A change control form is created for any system changes and completed forms are held and monitored in a manual filing system. A log of change control forms is now maintained.

### AXON online system

- Harvey Walsh has developed and built a new a model for the AXON backend database in discussion with the DARS team. The model includes data that is aggregated and the appropriate small number suppression. The solution has been built and tested by Harvey Walsh. The DARS team have signed off the AXON model that it meets NHS Digital requirements.
- A web application security assessment was carried out on the AXON application using dummy data on the 19 January 2017, followed by two retests on the 31 January and 1 February 2017 by an independent third party.
- Harvey Walsh informed AXON customers that the system will be offline on the 5 September 2016 and were given permission by NHS Digital to bring the AXON system back online on the 8 February 2017.
- Harvey Walsh was given permission by NHS Digital to bring the AXON system back on line on the 8 February 2017, when a new DSA was signed after issues identified in this audit and by the DARS team had been satisfactorily addressed.
- Harvey Walsh has purchased and transferred the hardware holding NHS Digital data from the third party to its own location.
- Data destruction certificates have been provided to the DARS team to support the destruction of the data on the backup server by the third party.
- An email was provided from the third party hosting company that old hard drives used to hold Harvey Walsh data (including NHS Digital data) had been decommissioned. There were no data destruction certificates available to support the hard disk destruction as Harvey Walsh had not requested the certificates at the time of when the hardware was decommissioned.
- Harvey Walsh has improved the password change control by implementing a system enforced password change for the AXON system.