Directorate / Programme	**Data Dissemination Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Terry Hill**	Version	**2.0**
Owner	**Rob Shaw**	Version issue date	**16/05/2016**

HSCIC Technical Audit: Methods Analytics

Contents

Executive Summary

This document records the key findings of a technical audit of Methods Analytics (Methods) following the Health and Social Care Information Centre (HSCIC) concluding the company had breached its Data Sharing Framework Contract and Data Sharing Agreement by holding and processing data outside of the UK. As a result of this breach Methods had been required to delete HSCIC record level data from its live systems.

The purpose of this technical audit was to examine the new storage and processing arrangements implemented by the company to address the cause of the breach prior to any decision being taken by HSCIC as to whether the company could start to receive data again.

Due to the nature of the audit, the process by which it was conducted and recorded differs from the published data sharing audits conducted by the HSCIC since August 2014. Specifically, this audit was conducted over an extended time-frame which allowed Methods to address comments and issues raised during an on-site visit, a review of two on-line tools and a review of documentation presented following the on-visit. As a result, conclusions are presented as statements rather than as non-conformities or observations based on the evidence presented during a site visit.

From the on-site visit and an independent review of Methods' online tools, further changes had to be made by Methods to address shortcomings identified by the Audit Team. Notably this has resulted in the majority of Methods' infrastructure being moved into two English datacentres and changes made to one of the online tools to improve small number suppression.

The Audit Team has concluded from this extended review that the storage and processing arrangements being established are reasonable for the nature of the data and have addressed the cause of the identified breach. However, as no data has yet been released to the organisation and therefore supporting evidence is lacking in some areas, a further audit is recommended. This further audit will also look at the results of penetration testing Methods will conduct once the environment has been finalised in terms of its design and operation.

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

1 About this Document

1.1 Introduction

The Review of Data Releases by the NHS Information Centre[1] produced by HSCIC Non-Executive Director Sir Nick Partridge recommended that the HSCIC 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, the HSCIC commenced a programme of external audits with organisations with which it holds data sharing agreements. The established audit approach and methodology is using feedback received from the auditees to further improve our own audit function and our internal processes for data dissemination to ensure they remain relevant and well managed.

1.2 Background

In November 2015 Methods was found to have breached its Data Sharing Framework Contract and Data Sharing Agreement with the storage and processing of both ONS and HSCIC record level data taking place within the Republic of Ireland, via Amazon Cloud Services. As a result of this breach the company was instructed by HSCIC to delete record level data from the Amazon servers.

The HSCIC declared in its notification letter dated 16th February 2016, that a detailed technical audit would be carried out of Methods' new processing and storage arrangements before being permitted to receive record level data under the existing agreement.

1.3 Purpose

This report provides an evaluation of how Methods has adapted its storage and processing arrangements in order to conform to the requirements of the Data Sharing Framework Contract and 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 of the new storage and processing arrangements, this report does not use the established approach taken to the reporting of data sharing audit findings (i.e. nonconformities and observations) since Methods had been given the opportunity to correct issues identified during the onsite visit and in subsequent desktop reviews. Section 2 does however present findings both from the on-site visit and at the time of writing in order to present a balanced view.

[1] www.hscic.gov.uk/datareview

1.5 Audience

This document has been written for the HSCIC Director of Data Dissemination Services and the Office for National Statistics. The report will be published in a public forum.

1.6 Scope

The audit considered the fitness for purpose of the new storage and processing arrangements being implemented by Methods and whether they posed any risk to patient confidentiality or to the HSCIC.

1.7 Audit Team

The Audit Team was comprised of senior certified and experienced ISO 9001:2008 (Quality management systems) and ISO 27001:2013 (Information security management systems) auditors and an information security subject matter expert.

2 Audit Findings

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

- an on-site visit to Methods' offices in Sheffield on 3rd March 2016 to examine the new storage and processing arrangements;
- desktop reviews of evidence, requested during the on-site visit, over the period 4th March to 5th April 2016; and
- a review of Methods' "Sword" and "Stethoscope" on-line tools to ensure that the level of suppression and re-identification were in line with the Hospital Episode Statistics (HES) Analysis Guide[2].

As no data has been cleared for processing and storage under the terms of the HSCIC notification letter, except for the provision of aggregate data in the on-line tools that existed prior to the breach being identified, the actual practices employed by Methods could not be fully audited. This restriction also acknowledges that the nature of the new environment changed as a result of the on-site visit and therefore implementation changes are in the process of being finalised.

2.1 Storage of Data

At the on-site visit, Methods declared that its customer facing tools would continue to be held on Amazon servers in the Republic of Ireland but the data processing would be carried out on servers located in Redcentric datacentres in England. The Audit Team stated that this arrangement was not as described on the data sharing application available at the on-site visit, in that the application omitted any reference to Amazon Web Services (AWS). The Audit Team stated the use of AWS needed to be discussed further with the HSCIC as this position was unacceptable. Notably, in its notification letter the HSCIC had stated the "application must be completely transparent in all detail, and cover the revised arrangements for storage and processing".

After subsequent discussions with the HSCIC, Methods has elected to migrate its Qlikview services to the English datacentres in order that all processing of data under the data sharing agreement will be within those datacentres. However, the company will continue to use AWS to support Stethoscope. Methods' rationale for this continuance is that only aggregated, small number suppressed data (anonymous data) is held or processed within Ireland. Importantly, Methods' application has been updated to reflect the continued use of AWS, which has been presented to the Data Access Advisory Group (DAAG).

[2] www.hscic.gov.uk/media/1592/HES-analysis-guide/pdf/HES_Analysis_Guide_Jan_2014.pdf

2.2 Access to Data

Methods stated there was an established process for notifying the IT team of any starters and leavers. New documentation has been created by the company to record access to HSCIC data. It is expected that such documentation will be created for staff requiring access in the future. Although a Data and Server Access Policy has been written, the processes it describes have yet to be fully implemented.

When someone leaves, the IT team is responsible for resetting passwords, deactivating customer record management accounts, barring access to all accounts and removing access permissions granted on company devices. The company acknowledged that any new processes for leavers would be included in its exit checklist which will be logged with HR.

Staff are issued with encrypted laptops. All devices used by staff have administrative rights for the local Windows machine. A record of this equipment is maintained on an asset register, which needs to be tightly controlled as the register contains the bit-locker keys for the assets. Methods confirmed that the asset register is only accessible by authorised IT staff.

Microsoft Intune[3] is used to manage and monitor user computers on a daily basis:

- Microsoft updates (including security and critical updates);
- Device encryption;
- Anti-Virus (Endpoint Protection built-in);
- Remote Wipe (used if device is lost or stolen);
- Password/Passcode compliance;
- Software inventory; and
- Removable device usage.

The environment to be housed in the Redcentric datacentres now includes the SQL servers and the Qlikview servers, as defined above. Copies of the initial and latest contracts with Redcentric were provided to the Audit Team.

Methods reported that four members of staff had a “Global Administrator” role, however, none of these staff had access or any control of the Redcentric environment. The company also confirmed that it does not have domain access in Redcentric.

Methods confirmed that all staff accounts are non-expiring and all accounts are to adhere to the stated password complexity and expiration group policies. Account lifetime is to be handled through defined management processes. Redcentric’s service accounts include non-expiring passwords.

[3] https://www.microsoft.com/en-gb/server-cloud/products/microsoft-intune/Overview.aspx

Remote access to the datacentre servers by Methods staff is controlled by appropriate authentication via a Redcentric VPN provision. Methods confirmed that all processing of record level data will be done within the datacentre. No record level data is to be saved to company laptops. Only aggregated data required for external reporting under the terms of the data sharing agreement will be saved locally.

Additional request forms, process documentation and reports have been created to define and manage individual access to servers following the on-site visit. Software added to the SQL servers in order to provide an auditable trial, has been tested and representative printouts were provided to the Audit Team. The continuation and availability of this management reporting for the final live system will be reviewed at a subsequent HSCIC audit.

A high level schematic for the new Redcentric environment showing how security will be enacted to ensure full protection of the internet facing elements in the datacentre was provided to the Audit Team on 4th April 2016. This schema showed a separation of the front facing and backend servers protected by firewalls. It is important for certain accounts and services to be isolated as some are hosting HSCIC data and some are internet facing. Due to the fluid nature of the environment the Audit Team has not reviewed the detail of the final configuration, just the declared logical architecture.

An independent application security penetration test was performed on the Stethoscope platform between 21st and 27th January 2015. Methods are currently in the process of resolving the identified issues. However, as the overall environment has changed significantly since this penetration test, in deed the design is still be finalised as a result of bringing the Qlikview servers into the English datacentre, Methods has confirmed that the company will perform a full penetration test of all SQL and Qlikview elements of the Redcentric environment once it is set up and working. The results of this penetration testing should be reviewed by the HSCIC once it has been performed.

At the request of the HSCIC an assessment of the servers using Microsoft Baseline Security Analyzer[4] was undertaken. Methods undertook this request on the SQL servers that were located in the Redcentric datacentre at the time of the on-site visit; the assessment did not include the Qlikview servers or the AWS servers. The limited analysis revealed a number of issues which have been classified by Methods as non-critical.

[4] https://www.microsoft.com/en-gb/download/details.aspx?id=7558

Independently, the HSCIC initiated a security audit of the Stethoscope tool using Nexpose[5]. The results of this analysis were provided to Methods to consider. HSCIC also strongly recommended that Methods take into account OWASP Application Security Verification Standard[6] Level 2 as a basis for its web application technical security controls.

2.3 Processing of Data

All processing of data is to be performed in the Redcentric datacentre over VPN with named accounts using two factor authentication.

The document "Secure Data Development Team Practices" has been established to define the approach by which software is developed and tested. This document may need to change to align with the final solution implemented by Methods. As no actual data is currently being processed, the Audit Team could only view a limited amount of evidence derived from the implementation of these procedures. More comprehensive evidence would be expected at a subsequent audit.

Data supporting Stethoscope's functionality will be processed in Redcentric and suppressed in line with HES Analysis Guide before it is transferred to AWS.

2.4 Transfer of data

In terms of its latest design, Methods confirmed that only anonymous data, in which low numbers have been suppressed, will be transferred to AWS. The table containing the anonymous, low number suppressed data will be backed up to Redcentric over a secure unidirectional VPN tunnel and then restored over S3 to the SQL database in AWS. This SQL database serves the web product "Stethoscope".

The other transfer of data is between the two English datacentres to back-up the data. Back-up is a managed service in which Methods configures the backups and undertakes the restores but the underlying infrastructure and support is provided by Redcentric.

2.5 Tool Review

A problem during a demonstration of Stethoscope during the on-site visit was noted by the Audit Team. Methods reported that this problem was probably due to a recent change to the software in the live environment. The company has since reported that the problem has now been fixed and tested.

[5] www.rapid7.com/products/nexpose

[6] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

In discussing the availability of data linked to a user's patients, Methods have stated that additional functionality is being developed to create an audit trail that Stethoscope users must use to record that the user has written permission in place. This change does not affect the established policy where any user requiring access to consultant level data in Stethoscope must obtain written permission from his/her Caldecott Guardian.

From an initial remote review of the Sword and Stethoscope tools it was found:

- Stethoscope was complying with the HES Analysis Guide in that it correctly suppressed small numbers; and
- the level of suppression in Sword was not adequate and did not comply with the HSCIC's suppression rules. In light of these issues, Methods has taken the tool off-line whilst fixes are made.

In support of the audit, Methods provided details on the data items used by the tools and where these items mapped to the supplied HES data.

At the time of writing this report, Methods is still working on ensuring that cross-tabulation analysis is suppressed and that any percentage figures are also suppressed where a denominator is present or it is clear that figures can be deduced.

The HSCIC to confirm that suppression in Sword is satisfactory before the output is made generally available.

2.6 Document Control

Some of the documents presented to the Audit Team had no, partial or inconsistent document management information, for example, version, date, author, approver and status. Methods recognised this issue and have updated some of the documents supplied to include document controls that were recommended by the HSCIC auditors in 2014.

The Audit Team would expect to see future documentation to have a correct and consistent approach to document management.

3 Conclusions

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

- findings from the on-site visit and tool review; and
- revised findings based on subsequent discussions and reviews.

The main findings are:

- at the on-site visit the storage/processing arrangements were found to be inconsistent with the data application which resulted in further equipment being relocated to two English datacentres. The design is still to be finalised;
- Methods is continuing to use AWS to host elements of its on-line service, importantly this arrangement is now clearly described in its latest application;
- new documentation has been created to support staff access to the data which also creates a chain of custody down to named staff;
- new processes have been developed to support the latest working environment. Whilst some evidence supporting their suitability was seen by the Audit Team, detailed evidence will not be available until the supply of record level data has been re-instated and the new data processed;
- Methods has installed audit software on the system to provide a local record of VPN and SQL data access;
- improvements are required to Sword to address HSCIC concerns over small number suppression and the ability to re-identify numbers; and
- Methods needs to improve its document management.

As the storage and processing arrangements were relatively new, there was a lack of evidence for some of the processes. It is proposed that a follow-up audit is conducted in a few months to review the final system configuration and to review evidence arising from the processes described by Methods and the records being generated by the system, for example access logs. This further audit will also look at the results of penetration testing Methods will conduct once the environment has been finalised in terms of its design and operation.

The HSCIC will also need to confirm that Sword conforms to the HES Analysis Guide once the software changes have been made and tested.

Notwithstanding the above statement, the Audit Team is content with the new storage and processing activities defined by Methods and subsequently updated following the on-site visit.