
| | | | |
|--------------------------------|-----------------------------|---------------------------|---------------------|
| Directorate / Programme | Data Dissemination Services | Project / Work | Data Sharing Audits |
| | | Status | Final |
| Acting Director | Chris Roebuck | Version | 1.0 |
| Owner | Rob Shaw | Version issue date | 19-Jan-2015 |

HSCIC Audit of Data Sharing Activities:

Methods Consulting

Contents

| | |
|--------------------------------------|-----------|
| Executive Summary | 3 |
| 1 About this Document | 5 |
| 1.1 Introduction | 5 |
| 1.2 Background | 5 |
| 1.3 Purpose | 6 |
| 1.4 Nonconformities and Observations | 6 |
| 1.5 Audience | 7 |
| 1.6 Scope | 7 |
| 1.7 Audit Team | 7 |
| 2 Audit Findings | 8 |
| 2.1 Access Controls | 8 |
| 2.2 Information Transfer | 8 |
| 2.3 Disposal of Data | 9 |
| 2.4 Risk Assessment and Treatments | 10 |
| 2.5 Operational Planning and Control | 10 |
| 2.6 Auditee Feedback | 11 |
| 3 Conclusions | 13 |
| 3.1 Next Steps | 14 |

Executive Summary

This document records the key findings of a Data Sharing Audit¹ of Methods Consulting on 22nd August 2014 against the requirements of the Health and Social Care Information Centre (HSCIC) Data Sharing Agreements (DSAs) in relation to data sharing agreement RU926 covering Hospital Episode Statistics (HES), Secondary Uses Service (SUS) for Payments by Results (PbR), Mental Health Minimum Data Set (MHMDS) and HES Provisional Major Care; all were provided in pseudonymised format. This audit was conducted using approved and mature methodology based on ISO standard 19011:2011 (Guidelines for auditing management systems) and follows the same format for all audits of Data Sharing Agreements conducted by HSCIC.

In total, four Minor Non-conformities and two Observations were raised²:

- There is a single point of failure due to only one named individual with access to securely stored data (Observation)
- The induction and development programme is informally managed (Minor)
- Documentation management and version control is poor (Minor)
- There is a lack of adequate procedural guidance for the destruction of data (Minor)
- Risk assessment is inadequate and the process is not fit for purpose (Minor)
- The internal audit programme is not informed by risk assessment and treatment reviews (Observation)

Areas of Good Practice

- Access Control and associated login methodology is managed
- Information passing over public networks is protected from fraudulent use, modification, disclosure, misrouting and duplication
- No direct link between public facing tools and information and source HES data
- Skills and knowledge of staff involved in the Data Sharing process
- ISO certification against three different standards (Quality Management, Information Security and Environmental Management)
- Processes and security measures for access and management of data using the Cloud environment³

¹ An audit is defined by ISO 9000:2014 as a *systematic and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled*

² Definitions found in Section 1.4

³ A Cloud environment deploys groups of remote server and software networks for centralised data storage and online access to computer services, often through the internet; this is generally to avoid upfront infrastructure costs.

In summary, it is the Audit Team's opinion that at the current time and based on evidence presented on the day, there is minimal risk of inappropriate exposure and / or access to data provided by HSCIC to Methods Consulting under the terms and conditions of Data Sharing Agreement RU926 signed by both parties.

1 About this Document

1.1 Introduction

The Health and Social Care Act 2012 contains a provision that health and social care bodies and those providing functions related to the provision of public health services or adult social care in England handle confidential⁴ information appropriately.

The Review of Data Releases by the NHS Information Centre⁵ 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 DSAs. 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.

Audit evidence was evaluated against a set of criteria drawn from the HSCIC's draft Code of Practice on Confidential Information⁶, DSAs signed by the relevant contractual parties and the international standard for Information Security, ISO 27001:2013.

1.2 Background

Methods Analytics was borne out of an approach by East Midlands Strategic Health Authority (SHA) to conduct a survey with hospital and Primary Care Trusts (PCTs) chief executives and medical directors across the Midlands to see what a Quality Observatory model would look like. Work was conducted across the Clinical Cabinet and range of services on the Midlands to collate and provide an overview of variations / trends in clinical care work streams.

The collated data were migrated to a data warehouse and the organisation began to subscribe to pseudonymised Hospital Episode Statistics (HES), Secondary Uses Service (SUS) for Payments by Results (PbR), Mental Health Minimum Data Set (MHMDS) and

⁴ Confidential information is defined by the Code of Practice on Confidential Information as data which:

- Identifies any person
- Allows the identity of anyone to be discovered, including pseudonymised information
- Is held under a duty of confidence

⁵ www.hscic.gov.uk/datareview

⁶ www.hscic.gov.uk/cop

HES Provisional Major Care data on a monthly basis. Following migration to new servers and ongoing receipt of monthly data, the organisation created queryable data through the development of a Structured Query Language (SQL) data warehouse in order to further develop and refresh queries on the monthly data received to provide improved services across the Midlands.

Methods' customers include England's National Health Service (NHS). The primary focus of the service provided is to make information available to the public and clinical practitioners. In particular, the aim is to use information to engage with clinicians and other health professionals in order to enable decision makers to improve clinical outcomes, quality of care and the safety of the NHS. Work to date has resulted in an Acute Trust Dashboard which provides information across six (6) domains of the NHS operating framework for all Trusts in England. This has evolved into a web tool called Stethoscope which now features information regarding Trusts and Clinical Commissioning Groups (CCGs) across England.

After the abolition of the Health Authority and subsequently Primary Care Trusts, the organisation was initially hosted by Greater East Midlands before ultimately becoming an independent commercial organisation known as Methods Analytics. At the time, all staff transferred to the new company.

1.3 Purpose

This report provides an evaluation of how Methods Consulting conforms to the requirements of DSA RU926 covering Hospital Episode Statistics (HES), Secondary Uses Service (SUS) for Payments by Results (PbR), Mental Health Minimum Data Set (MHMDS) and HES Provisional Major Care; all were provided in pseudonymised format. It also considered whether Methods conformed to its own policies and procedures. This document provides a summary of the key findings.

1.4 Nonconformities and Observations

Where a requirement of either the DSA or the audit criteria was not fulfilled, it will be classified as a Major Nonconformity, Minor Nonconformity or Observation.

1.4.1 Major Nonconformity

The finding of any of the following:

- The absence of a required process or a procedure
- The total breakdown of the implementation of a process or procedure
- The execution of an activity which could lead to an undesirable situation
- Significant loss of management control
- A number of Minor Nonconformities against the same requirement or clause which taken together are, in the Audit Team's considered opinion, suggestive of a significant risk

1.4.2 Minor Nonconformity

The finding of any of the following:

- An activity or practice that is an isolated deviation from a process or procedure and in the Audit Team's considered opinion is without serious risk
- A weakness in the implemented management system which has neither significantly affected the capability of the management system or put the delivery of products or services at risk
- An activity or practice that is ineffective but not likely to be associated with a significant risk

1.4.3 Observation

In the Audit Team's considered opinion, a situation where a requirement is not being breached but a possible improvement or deficiency has been identified.

1.5 Audience

This document has been written for the Director of Data Dissemination Services. A copy will be made available to the HSCIC Community of Audit Practice, Assurance and Risk Committee and the Information Assurance and Cyber Security Committee for governance purposes. 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 Methods Consulting along with its associated documentation.

Fundamentally, the audit sought to elicit whether:

- Methods Consulting is adhering to the standards and principles of the DSA and audit criteria
- Data handling activities within the organisation pose any risk to patient confidentiality or 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.

The audit was conducted in accordance with ISO 19011:2011 (Guidelines for auditing management systems).

2 Audit Findings

This section presents the key findings arising from the audit.

2.1 Access Controls

Methods Consulting has established a management framework to control the implementation and use of data received from HSCIC. An Information Security Policy is in place with named senior officers within the organisation responsible for adherence to this policy. Employees with specific responsibilities for receipt and management of data are required to complete mandatory Information Governance (IG) training on an annual basis.

All employees are put through an informal induction programme and on the job training at corporate and business unit level. Consideration needs to be given to formalising an induction and development programme for all staff.

The password protection procedure requires changes every 30 days.

Evidence was provided to demonstrate that only the staff named within the DSAs had access to data provided by HSCIC. Access is through a secure login protocol which provides an audit trail of activity. Security screening of all staff is also in place prior to them being given access to the data warehouse and stored data files. The Asset Register and encryption methodology / tool is fully utilised with recovery key information locked down and accessible by only two members of Methods staff. A Starter and Leaver Checklist is in place and has controlled management arrangements which includes removal of names.

Secure access to HSCIC file transfer protocol (ftp), which is then loaded into the Cloud environment, is granted to only one named individual within the organisation. This, however, presents a single point of failure and Methods Consulting should consider competency development for other named and suitably qualified staff. This information is to be recorded on the DSA.

The public facing web portal provides only Trust level aggregated data through a Quality Dashboard as a snapshot of information at any given point in time. Methods' clients wishing to access NHS sub-Trust-level information can only do so through a subscription model. The tool is monitored by specific software to ensure security of data and audit trails of access.

Conclusion: Access Control and associated login methodology used to gain access to public facing and secure data seems well managed and there appears to be minimal risk of exposure to unauthorised / inappropriate access to data.

2.2 Information Transfer

Received information is initially collated in a secure server before being transferred to the virtual environment. All testing and development of data models for use by

subscribers and / or public view is managed in the secure environment and taken through a Quality Assurance process prior to release. The testing process was demonstrated and found to be sufficiently secure.

The public facing web portal provides only aggregated data through a Quality Dashboard as a snapshot of information at any given point in time. Methods' clients wishing to access NHS Trust-level information can only do so through a subscription model. Subscribing organisations must submit the names of those employees who have been authorised to access Trust-specific information.

All Small Numbers⁷ which may identify an individual are suppressed.

Conclusion: Information passing over public networks is protected from fraudulent use, modification, disclosure, misrouting and duplication. There is no direct link between public facing tools and information and the source HES data which is managed on a separate secure environment.

2.3 Disposal of Data

The DSA specifically refers to a requirement to provide confirmation in writing of secure disposal.

Although a documented procedure for the import of HES data has been written, it lacks configuration management and version control. In addition, the step around disposal of data does not provide specific instructions on how this is to be managed other than deleting from a shared drive; there is no reference to ensuring any other versions or copies are deleted from other and / or personal drives. Risks are minimal due to HES data being processed in a single Cloud environment and not on personal drives. Further, there is no stated requirement to provide written confirmation to HSCIC that data has been securely disposed.

The document does not state that deletion from a shared drive means back-ups have also been deleted. There is no instruction to ensure that back-ups are also erased although confirmation was provided that destruction of back-up files also includes any earlier copies of stored back-ups.

Records of destruction are auditable through the internal user and activity logs available through the system. However, due to time constraints, the audit team did not see evidence; this will be followed up at the next audit visit.

⁷ Up to 5 individuals

Conclusion: The safe handling of information from import to disposal, including record keeping, can be improved although no risk to data has been noted due to the skills and knowledge of staff involved in this process complemented by the access controls. This will be addressed as a priority area for follow-up at the next audit.

2.4 Risk Assessment and Treatments

A Risk Register is in place as required by the DSA. However, this is considered by the audit team to be a major area for improvement.

- Version control is missing
- No matrix is in place: the impact is noted but no likelihood of the risk occurring is recorded
- The same risk is listed on more than one occasion but with different risk identification numbers
- The log is reviewed on an annual basis only which is insufficient to ensure appropriate controls
- There is a lack of mitigating actions and documented evidence of management review and control
- There is a lack of Risk / Action Owners and timescales for resolution
- An audit programme was seen to be in place however the areas are cyclical and regular instead of being informed by risks to the organisation and the consequential potential impact

Conclusions: There is no comprehensive end to end risk assessment and treatment process. This needs to be addressed as a priority area for follow-up at the next audit.

2.5 Operational Planning and Control

The organisation is ISO certified to three standards: 9001:2008 (Quality management), 27001:2013 (Information security) and 14001:2004 (Environmental management). An in-house lawyer conducts reviews to ensure compliance with regulatory changes and disseminates any potential implications across the organisation.

A Business Continuity Plan is in place with a virtual Business Continuity team. Methods currently employ a consultancy-based service to inform IG compliance. Consideration should be given to development of in-house provision in order to reduce risk and improve career path opportunities.

All development and analysis arising from products using source data is Quality Assured through the Senior Analyst.

Methods have an internal audit programme in place confirmed by ISO 9001 surveillance visit (please refer to [Section 2.4](#) for qualifying statement).

The following documented policies were stated as being in place but not seen by the Audit Team due to time constraints; they will be assessed at the next visit:

- Access control
- User registration process
- Mandatory IG and IG refresher training for all staff
- Guidance handbooks in place for standards processes and procedures used by the organisation
- Minutes for monthly management meetings
- Annual Business Plan
- Information Asset Register
- Statement of Applicability

Conclusions: ISO certification against three different standards (Quality Management, Information Security and Environmental Management) indicates independent validation of control effectiveness. An internal audit programme is in place but requires further development through an informed risk management methodology.

2.5.1 Virtual Cloud Environment

Data and products are held in a virtual Cloud environment. At the time of the visit, no verification of security integrity was available; this has been subsequently provided.

It is noted that data is not held in any physical devices and as such, there is no possibility that such devices containing data can be lost. All of the layers of security ensure the Cloud is extremely difficult to access and would pass stringent 'motivated invader' tests. Cloud-based service provision is ISO 27001 compliant. Methods employ responsible and secure processes to ensure appropriate access and management of data held in the Cloud environment.

Access to the Cloud is granted to only one named individual within the organisation. This, however, presents a single point of failure and Methods Consulting should consider competency development for other named and suitably qualified staff. This information is to be recorded on the DSA.

Conclusions: Current Methods' processes and security measures for access and management of data using the Cloud environment seem fit for purpose and well controlled.

2.6 Auditee Feedback

Methods Consulting was provided with an opportunity to comment on any aspect of the current processes employed by HSCIC in disseminating data, the DSA or the audit itself.

2.6.1 ONS Data

ONS data is received and being used in-house to replicate the Summary Hospital-level Mortality Indicator (SHMI) type data repository. Methods request that an agreement is developed to allow use of the data to enable modelling of SHMI type information for use by NHS subscribers. The development of such a product based on source ONS data which is held on a separate secure environment would provide information at sub-Trust level.

2.6.2 Copyright

Clear guidance is required from HSCIC over positioning of copyright recognition and source of data (i.e. front screen / pages only or all screens and pages of all products).

2.6.3 DSA Applications

Clear guidance from HSCIC is required to explain the rationale and approach to take completing the DSA application. For example, the term “Researcher” is not explained.

There is an inconsistent application of the subscription period of the DSAs / Data Sharing Re-use (DSR). Burden on both sides is therefore more onerous than would be necessary if agreements / renewals covered a 12 month period as a minimum.

2.6.4 Data Transfer

Clear advice is required with regards to acceptable software which can be used for the secure transfer of data to / from HSCIC.

2.6.5 Governance

Governance arrangements which oversee release of data by HSCIC must be finalised and communicated to interested parties.

3 Conclusions

Table 1 identifies the Major and Minor Nonconformities and Observations (Obs) raised as part of the audit.

| Ref | Comments | ISO 27001 Clause | Section in this Report | Designation |
|-----|---|------------------|------------------------|-------------|
| 1 | There is a single point of failure due to only one named individual with access to securely stored data | 9.1 | 2.1 | Obs |
| 2 | The induction and development programme is informally managed | 7.3 | 2.1 | Minor |
| 3 | Documentation management and version control is poor | 7.5.2 b | 2.3 | Minor |
| 4 | There is a lack of adequate procedural guidance for the destruction of data | 6.1.1 | 2.3 | Minor |
| 5 | Risk assessment is inadequate and the process is not fit for purpose | 6.1.2 | 2.4 | Minor |
| 6 | The internal audit programme is not informed by risk assessment and treatment reviews | 9.2 | 2.5 | Obs |

Table 1: Nonconformities and Observations

3.1 Next Steps

Methods Consulting is required to review and respond to this report, providing corrective action plans, the parties responsible for the action and the timeline, based on priority and practicalities for incorporation into existing workload. As per agreement, management response will be discussed by the Audit Team and validated at a follow-up meeting with Methods Consulting to confirm whether the proposed actions will satisfactorily address Nonconformities and Observations raised.

Ongoing monitoring of progress against corrective actions will be conducted to an agreed schedule with Methods Consulting.