Data Sharing Audits: A Guide for Data Recipients

Ensuring recipients of our confidential information are committed to its safe handling

Version 1.0

Published 18 October 2016

Information and technology
for better health and care

Contents

Information and technology
for better health and care

1 Introduction

1.1 Why is NHS Digital conducting data sharing audits?

Under the Health and Social Care Act 2012, the Health and Social Care Information Centre (also known as NHS Digital) has a legal duty to maintain the confidentiality, safety, security and integrity of all personal and patient data it holds and disseminates.

NHS Digital provides confidential information to a wide variety of organisations to support specific purposes. Each data dissemination is subject to a data sharing framework contract and data sharing agreement. The purpose of a data sharing audit is to ensure that the data recipient is meeting the requirements of the data sharing framework contract and data sharing agreement, along with other relevant standards and guidelines.

In August 2014, NHS Digital began auditing organisations with which it holds data sharing agreements to ensure that confidential information is handled appropriately.

1.2 Who is this guide for?

This guide is designed for all recipients of data from NHS Digital under a data sharing framework contract and data sharing agreement for the purposes of benefitting health and social care. It is designed to provide an understanding of NHS Digital's management of the data sharing audit process so that:

- data recipients understand how NHS Digital will approach an audit; and
- there is enhanced public trust in one of the ways in which NHS Digital maintains security of the data provided to data recipients.

2 The data sharing audit process

This section guides the data recipient through the various stages of a data sharing audit. Whilst all of the stages described will generally apply, in certain instances some stages may not be relevant.

2.1 The Audit Team

NHS Digital has established an independent audit function, separate from those NHS Digital teams responsible for the release of data, specifically to audit data sharing applications, framework contracts and agreements.

Audit Team personnel are suitability experienced and hold internationally recognised qualifications such as: Lead Auditor/Auditor ISO 9001:2008 (Quality management systems), Lead Auditor/Auditor ISO 27001:2013 (Information security management systems), Certificate Information System Auditor (CISA) or Masters in Information Rights Law and Information Governance.

For certain audits, the Audit Team may include Subject Matter Expertise to ensure the necessary balance of expertise and competence.

2.2 How is an organisation selected for audit?

Data recipients should expect to be audited at least once in a three year period. However, some organisations may be subject to additional audits based on a risk profile derived from one of more of the following criteria:

- NHS Digital has received complaints about a data recipient;
- there are known issues or concerns which may have been raised externally, for example, by a whistle blower, another organisation or an independent body;
- a repeat extension for the same data has been received by NHS Digital;
- there are concerns over the IG Toolkit score;
- an organisation has many different data sharing agreements for different datasets or cuts of data and therefore there is a risk of linking / identification; or
- NHS Digital seeks confidence in an organisation's ability to handle data securely as part of the data sharing application stage.

2.3 Types of data sharing audits

A data sharing audit will fall under one of the following five types:

1. **Routine** - A data sharing audit of an organisation already in receipt of data which will look at the full range of topics listed in section 2.4. The data recipient will receive a reasonable amount of notice as described in section 2.5. Depending on the nature of the findings identified, a post audit review may be conducted, see section 2.16.

2. **Focused** - This audit is similar to a routine audit but will focus on specific elements (for example, data destruction). As a result of the tighter scope, the onsite visit will generally be shorter than for a routine audit however the reporting and post audit review will be the same.
3. **Pre-release** - An audit that has been requested when NHS Digital seeks confidence in the organisation's ability to handle data appropriately prior to any release. This type of audit will normally look at the full range of topics listed in section 2.4. A post audit review may be conducted (see section 2.16) depending on the nature of the findings identified. The need for a post audit review may delay the application process.
4. **Heightened concern** - This audit will be conducted on an organisation that has been subject to scrutiny by NHS Digital. This scrutiny may result following an incident and suspension of access to data. The audit is designed to determine whether the data recipient has enhanced its controls and is now in a position to start receiving data again. The approach of this type of audit may differ from the above audits in that it may combine both onsite elements and post audit review activities in order to fully conclude whether the organisation should receive data. The results may be presented in the audit report in a different format as to the above audits as a result of these combined activities.
5. **Unannounced** – Similar to a routine or focused audit, except that no notice will be given to the data recipient. This type of audit will only be undertaken when special circumstances exist.

2.4 Scope of a data sharing audit

The scope of an audit will consider the fitness for purpose of the main processes of data handling at the organisation along with its associated documentation. The ready availability of suitable evidence will play a key part in the audit.

Fundamentally, the audit will seek to determine whether:

- the organisation is adhering to, or has the ability to adhere to, the requirements of a data sharing framework contract and a data sharing agreement(s);
- 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.

The scope areas usually considered by the Audit Team are:

- information transfer;
- access control;
- use and benefits of data;
- data destruction;
- risk management; and
- operational management and control.

Typical questions and evidence related to these scope areas are described further in Appendix A.

2.5 Informing an organisation of an audit

Once an organisation has been scheduled for an audit, the assigned Lead Auditor will send a notification letter to the data recipient's main contact. This notification letter will be sent by email no less than 10 working days prior to the proposed audit date. For an unannounced audit there will be no notification letter and no prior notice.

In the notification letter a date for the audit will be proposed based around the defined NHS Digital programme of data sharing audits. Whilst the Lead Auditor would seek to maintain this date, it is recognised that the date may not always be convenient to the data recipient. In this case the Lead Auditor will discuss any request to change the date with the data recipient and may amend the date.

A draft audit plan (Appendix B) will be provided by the Lead Auditor along with the notification letter. This plan will be tailored to meet the specific scope of an audit.

The Audit Team will require access to managerial, operational and technical personnel who are able to cover the breadth of the areas detailed in Section 2.4 which are covered by the scope of the audit. These representatives may be from Information Governance, Information Security, Information Technology, Human Resources and Business Intelligence, but this will depend on how the organisation is structured.

The Lead Auditor will contact the data recipient's main contact prior to the audit to:

- agree locations for the onsite visit and the duration of the audit. The onsite visit may include separate locations where data is held, for example, in separate data centres;
- discuss the Audit Plan to ensure that an appropriate mix of staff will be available to support the audit; and
- identify and agree any policies and procedures that could be provided in advance of the onsite visit.

Prior to the onsite visit, the Audit Team will liaise with NHS Digital colleagues to gain background and information on general themes / concerns about the organisation. For example, the Audit Team may commission a desktop review of any submission using NHS Digital's IG Toolkit where applicable.

2.6 What material will the Audit Team want to see?

In the notification letter, the data recipient is asked to provide the policies and procedures that cover the scope of the audit in advance of the onsite visit. Representative policies and procedures are shown in Table 1. However, as document titles vary across organisations, it is the responsibility of the data recipient to identify and supply relevant existing material. Further examples of documentation are given in Appendix A.

Employee Awareness and Training	Data Disposals Policy
Information Governance Policies	Mobile Computing Policy
Password Policy	Back-up and Recovery Policy
Acceptable Use Policy	Retention / Records Management Policy
Encryption Policy	Network Management Policy
User Management Policy	Confidential Data Policy
Information Handling Policy	Remote Access policy
Data Protection Policy	Incident Management Policy
Network Security Policy	Risk and Issue Management Policy

Table 1: Representative Policies

These documents will be used to inform the direction of the audit and will be reviewed at NHS Digital offices prior to the onsite visit.

All of the material supplied by, or on behalf of, a data recipient will be held securely with access limited to the Audit Team, support personnel and its management team. All NHS Digital staff with access to the material are cognisant of their obligation to keep this information safe and confidential.

The material supplied by, or on behalf of, the data recipient will be used by the Audit Team to support the production of the audit findings within in the Data Sharing Audit report.

Once the Audit Team has determined that the retention of this material is no longer required for the purpose it was supplied, it will be deleted from the NHS Digital's secure server and NHS Mail or shredded if supplied on paper. Generally, this destruction will be shortly after the audit report has been published online. The Audit Team may elect to keep material relevant to a nonconformity until publication of the post audit review report.

Material to be destroyed when no longer required will include:

- all emails relating to the audit irrespective of their source, except for the email which confirms the accuracy of the draft report by the data recipient;
- documentation supplied by, or on behalf of, the data recipient;
- written notes taken by the Audit Team; and
- draft versions of the audit report created by the Audit Team.

NHS Digital may receive requests under the Freedom of Information Act 2000 to disclose information in relation to an audit. All requests for information are looked at on a case by case basis by the appropriate team within NHS Digital. This team may consult with the organisation in question before responding to the request.

2.7 The onsite visit

The onsite visit will usually take two days and involve two auditors; the actual number of days and team members will be confirmed in the draft audit plan sent with the notification letter. The Audit Team will try to keep disruption to the organisation to a minimum through the agreement of the audit plan.

Where possible, a room should be made available at sites identified in the audit plan for NHS Digital's auditors to carry out interviews when it is not appropriate to work 'desk side' or while they review material. Internet access is not required.

At the start of the visit, the Audit Team will hold an opening meeting with appropriate representatives of the organisation to explain the audit process. This meeting also provides an opportunity to discuss any issues or concerns. The Audit Team may make simple changes to the audit plan at the opening meeting should the need arise.

While onsite the Audit Team will meet with representatives of the organisation to establish if appropriate controls are in place and proactively followed to ensure that NHS Digital data sharing requirements are met. The approach used by the Audit Team is primarily evidence-based through interview.

Interviews will be supplemented by visual inspections of documents, records and uses of data within the organisation as well as other areas which are in scope such as access controls and storage solutions.

The Audit Team will require access to relevant operational staff where possible to understand how staff process data supplied by NHS Digital.

The questions asked and evidence gathered will depend on the scope of the audit and upon any specific requirements of the data sharing agreement(s). However, there are some generic areas which are normally covered during an audit. Examples of these areas are contained in Appendix A.

During the onsite visit, the Audit Team will make and retain notes from interviews, observations and testing. Copies of any policies or procedures not supplied prior to the audit visit may also be requested by the Audit Team. In most instances the Audit Team will not retain or distribute paper copies, particularly when the organisation has declared the material to be confidential. Any documentation that is taken away will be handled appropriately by the Audit Team. Documentation will be securely destroyed by the Audit Team when it is no longer required (see section 2.6 with respect to the retention of information).

From the perspective of the Audit Team, the most important element of an audit is that access to evidence is provided by the data recipient and questions are answered openly, comprehensively and accurately.

The Audit Team will hold a closing meeting with the organisation's representatives. Findings which have been identified by the Audit Team will be highlighted at this meeting in the form of nonconformities, observations, follow-up and good practice.

The Audit Team may also request additional pre-existing evidence that was unavailable at the onsite visit to be supplied within five working days of the visit. Therefore, findings may change as result of the review of that evidence. There could also be occasions where issues come to our attention after the onsite visit that the Audit Team may include in the audit report. The Lead Auditor will inform the key contact of any such changes. The Audit Team will not review material generated or updated after the onsite visit; such material may be reviewed as part of a post audit review.

Any material considered important by the Audit Team that could not be provided in a timely manner will be identified in the audit report as "follow-up". Such material would be reviewed by the Audit Team as part of a post audit review. At this time further nonconformities or observations may be raised against this material.

2.8 Nonconformities and observations definitions

Where a requirement of the data sharing framework contract, data sharing agreement or the data recipient's own documentation was not fulfilled, it is classified as a major nonconformity or minor nonconformity. Potential deficiencies or areas for improvement are classed as Observations.

Major nonconformity

The finding of any of the following would constitute a major nonconformity:

- significant failure to implement a requirement such as contained within a contract or agreement;
- 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; or
- a number of Minor Nonconformities against the same requirement.

Minor nonconformity

The finding of any of the following would constitute a minor nonconformity:

- limited failure to implement a requirement such as contained within a contract or agreement;
- 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; or
- a weakness in the implemented management system which has neither significantly affected the capability of the management system nor put the delivery of products or services at risk.

Observation

An observation is a situation where a requirement is not being breached but a possible improvement or deficiency has been identified by the Audit Team.

2.9 Assurance rating definitions

The Audit Team will assign an assurance rating to each of the scope areas examined based upon the findings of the audit. Ultimately an assurance rating is a measure of the control the organisation has within the scope area, with specific regard to the fitness for purpose of the data recipient's main processes of data handling and the application of this control by staff.

Substantial assurance	Detailed processes and procedures are in place and there is strong evidence that staff are following them. The audit may have identified limited scope for improvement in the existing arrangements.
Moderate assurance	Processes and procedures are in generally place, existing procedures may require some attention and there is evidence of compliance. The audit has identified some scope for improvement in existing arrangements
Limited assurance	There are insufficient processes and procedures, or they require substantial improvement or staff are generally not aware/following.
Unsatisfactory assurance	Processes and procedures are absent; those that do exist are generally weak or the processes are not being followed.

Table 2: Assurance ratings

2.10 Risk Statement

The Audit Team will provide an overall risk statement based upon the evidence presented during the audit and the type of data being shared at the time of the audit. The Audit Team opinion will be based upon the scale of the 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.

The risk statement will be based on:

- the nature of the data in terms of potential identification from those data items could cause harm or distress;
- the soundness of the organisation's control (as reflected in the assurance statement); and
- the context in which the data is being used.

The risk will be expressed as:

- Low;
- Medium;
- High; or
- Critical.

2.11 Draft and final reports

A draft audit report will be issued to the data recipient within the timescale stated in Table 3. The report will present the specific nonconformities and/or observations as described at the closing meeting and amended following the review of any material requested by the Audit Team and provided shortly after the onsite visit.

Although the Audit Team will consider all of the areas within the scope of the audit, the report is an exception report based on the criteria expressed in section 2.4. The audit report will also identify areas of good practice demonstrated by the data recipient.

The data recipient is requested to check the draft audit report for factual accuracy or commercially confidential information it feels should not be included. The data recipient should return its feedback and/or any suggested amendments to the Audit Team in accordance with the requirement shown in Table 3.

Should the data recipient not respond within the stated timescale, it will be deemed that it has accepted the report as factually accurate. If an organisation requires additional time to consider their response, it may request an extension from the Audit Team.

All factual inaccuracies will be amended by the Audit Team. Although rare, disagreement between the two parties may occur regarding the findings. Whilst it is a matter for NHS Digital to determine the content of the final report, where there is a non-resolvable disagreement between the Audit Team and the data recipient then an appropriate comment will be added to the report to reflect the data recipient's opinion. See also Section 2.17.

By its very nature, a two day audit of an organisation processing data cannot be deemed to be conclusive. Final report findings should always be viewed in this context. A positive final report is indicative of a level of assurance regarding a data recipient's policies and procedures at a certain point in time in relation to the agreed scope areas.

2.12 Publication

The data sharing audit report will be published on the external NHS Digital website. Audit reports are scheduled to be published on the third Thursday of each month.

The Audit Team will inform the data recipient at least one week prior to when the report will be made available on the external website. The NHS Digital Communications Team may use NHS Digital's Twitter account to publicise that the audit report is available online.

Currently the website on which reports can be accessed is: http://digital.nhs.uk/dsa.

2.13 NHS Digital action resulting from an audit

Findings that present a serious divergence from the contract and agreement or those findings which present an unacceptable risk to NHS Digital or to its stakeholders (including patients), will be addressed directly by the NHS Digital department responsible for the release of data.

A decision will be made by the Senior Information Risk Owner or Director of Data Dissemination Services on the course of action to take in response to any identified nonconformities.

2.14 Data recipient response to findings

The audit report may require a data recipient to provide a plan which details the action to be taken, the name of the party responsible and the timeline set for each action. It is the responsibility of the data recipient to decide on an appropriate course of action and ensure it addresses the nonconformities and observations.

In addressing a finding the data recipient must take account of any referenced supplementary notes presented in the audit report. The data recipient may use its own action plan template or the template provided in Appendix C.

The data recipient will be required to send the action plan to the Lead Auditor no later than the timescale specified in Table 3.

2.15 Timescales

The following table presents the expected timescales for the audit process; however these timings will be dependent upon the outcomes of any audit and are subject to change.

Action	Responsibility of NHS Digital	Responsibility of data recipient
Send out notification letter and draft audit plan	Minimum of 10 working days prior to proposed audit date	
Completed audit plan returned to Lead Auditor		5 working days prior to proposed audit date
Onsite visit	Agreed audit onsite visit date	
Draft audit report issued to data recipient for comment	Within 10 working days following onsite visit	
Draft audit report returned to Lead Auditor with comments		Within 10 working days of receipt of draft audit report
Final audit report published on NHS Digital website	3rd week of month	
Data recipient provides NHS Digital with action plan to audit report		Within 10 working days from publication of audit report

Table 3: Audit Timings

2.16 Post audit review

Where an action plan has been requested in an audit report, then the actions shall be assessed as part of a post audit review. A post audit review may also be undertaken when the report identifies issues not covered during the audit.

Wherever possible, the Lead Auditor will be responsible for any post audit review. Where this is not possible, the review will be delegated to the accompanying auditor. A review of the data recipient's action plan and suitable supporting evidence to demonstrate the action is working and is effective will be undertaken.

NHS Digital will contact the organisation, usually by email, to request an update on progress of the action plan items within timescales shown in Table 4, taking into account individual completion dates of required action declared by the data recipient.

Most significant finding in audit report	Expected timing of follow-up by NHS Digital
Major nonconformity	0 - 3 months
Minor nonconformity	3 - 6 months
Observations	At the discretion of the Lead Auditor, in accordance with any statement in the audit report

Table 4: Expected post audit review timescales

The type of post audit review activities undertaken will be determined by the overall findings of the data sharing audit, the resulting actions and the nature of the evidence supporting the actions.

The review may comprise:

- an independent desktop review of the evidence;
- a telephone / conference call to walk through the evidence;
- a WebEx session so that evidence held on the organisation network can be presented; or
- a further onsite visit.

A draft post audit review report will be written following the review conducted. The report will be produced in the same way as the audit report and will detail progress taken to address the findings raised. The NHS Digital will highlight any serious concerns in relation to any nonconformities which have not been addressed.

The process of publishing this report will be the same as the audit report.

2.17 The data recipient experiences an issue

If the data recipient has an issue with any aspect of the audit process, then the issue should be raised directly with the Lead Auditor. Where the Lead Auditor does not resolve the issue satisfactorily, or in a timely manner, then the data recipient may raise a formal complaint.

The NHS Digital complaints procedure can be found at:
http://digital.nhs.uk/article/1988/Making-a-complaint

2.18 Providing feedback

Feedback received from data recipients is used to further improve our audit process to ensure it remains relevant and well managed. A data recipient will be sent an evaluation questionnaire, or in some cases telephoned, once the audit report has been made publicly available.

Feedback from completed questionnaires will be analysed by a team independent of the audit function and the overall results made available to the Audit Team to consider the findings.

Appendix A Examples Of Evidence

This appendix describes the type of questions and typical evidence related to the area of scope considered on a data sharing audit, highlighted in Section 2.4. The purpose of this appendix is to help the data recipient prepare for the audit and to identify suitable representatives to meet the Audit Team.

Within the scope of the key objectives, the Audit Team is free to explore any aspect in detail to assure itself that appropriate controls are in place and that there is suitable evidence to demonstrate the controls are being followed.

The following table provides an example of evidence which the Audit Team may wish to view. It should be noted that other sources may be requested by the Audit Team to support the audit. Note that whilst similar evidence may be listed under more than one area, the organisation will only be required to supply this once.

Information transfer	
Typical opening questions/requests	**Examples of evidence**
• Describe the organisation's infrastructure and the interfacing to any relevant third parties. • How does data flow around the whole infrastructure and specifically where does data reside? • How does the organisation ensure any information passing over public networks is protected from fraudulent use, modification or disclosure? • How long will data be resident and what processes are in place to review its retention? • Is data processing/storage in line with the data sharing framework contract or agreement? • Is there a suitable contractual relationship with any 3rd parties? • Are technical reviews carried out when platforms are changed?	• Information flow mapping • Information security policies and guidance • Storage and backup policies • Contract/agreements with any data processors or third party data centres • Sub-licencing arrangements

Access control	
Typical opening questions/requests	**Examples of evidence**
• What are the physical security measures in place within offices and data centre(s), where appropriate? • Is suitable access only available to recognised / approved users for each of the touch points identified under information transfer? • Is access amended in the event of personnel changing roles? • Is appropriate penetration testing undertaken by the organisation?	• Account protection including organisational IT infrastructure, for example, firewall, encryption, anti-virus / anti-malware and patching policies • User / customer access permissions • Authentication process including logging and monitoring • Hardware and mobile device allocation and encryption • Joiners, leavers and movers processes • Information security policies • Sub-licencing arrangements • IT system and access change management process and tools • Password policy and processes • Physical building access controls • Remote access policy • Guest access policy • Security audits • Physical and environment controls around the storage of data (server rooms and data centre • External and internal penetration tests

Use and benefits of data	
Typical opening questions/requests	**Examples of evidence**
• Is the data is being used in accordance with the agreed purpose? • Are the declared benefits being achieved? • Has the organisation recognised NHS Digital's copyright, when appropriate?	• Publications and research papers • Analytical software / tools • Sub-licencing arrangements • Operating procedures

Data destruction	
Typical opening questions/requests	**Examples of evidence**
• Is there an established framework for the destruction of data and the media on which data is recorded (paper and electronic)? • Are decommissioned assets held in a secure area until destroyed? • How are assets destroyed? • Is a suitable 3rd party used to destroy assets? What records are produced to demonstrate that the assets have been destroyed? • How is the destruction of an asset linked back to the asset log? • Have Data Destruction Certificate(s) been returned to NHS Digital?	• Information asset register • Equipment asset register • Data disposals policy and processes • Contract / service level agreement with any third party disposal company • Disposal log • Certificates of destruction from disposal company • Destruction of paper based information records

Risk management	
Typical opening questions/requests	**Examples of evidence**
• Does the organisation have a formal risk and issue management process? • Are risks to data assets assessed to ensure that data is secure? • Have additional controls to unacceptable risks been identified and implemented? • Is there evidence to show that risks are periodically reviewed to ensure that controls remain relevant and effective?	• Risk management framework / procedure • Risk register(s) and associated controls • Risk assessments / mitigation • Privacy impact assessments • Minutes of management meetings

Operational management and control	
Typical opening questions/requests	**Examples of evidence**
• How does the organisation remain compliant with legal and contractual requirements? • What is the organisation's information security and information governance assurance process(s)? • Who has responsibility to manage and control information governance processes? • How are new and updated policies/processes communicated to all staff? • Does the organisation have an internal audit programme in place? • Is security testing conducted by the organisation? • How does the organisation identify and manage its information and equipment assets? • How does the organisation manage and report incidents? • Does the organisation have policies and procedures related to configuration control, patch management, asset management in place? • Does the organisation have an established information governance training programme, which includes refresher training?	• Information Security Policy and Information Governance Framework • Information governance policies • Evidence of Senior Management ownership of information governance • Minutes of meetings • Disaster recovery plan • Business continuity plan and tests • Change management processes and any associated tools • Policies, procedures and tools related to configuration control, patch management, asset management, media handling and change management • Incident management processes and any associated tools • Information asset register, identifying Information Asset owners • Equipment asset register • External and internal audit plans and audit reports, covering IT Security and Information Governance in the area in scope of the audit • Security assessments, including external and internal penetration tests • Employee awareness and training policies, including information governance training materials and training records for both staff induction and refresher training • Sub licencing arrangements

Appendix B Representative NHS Digital Audit Plan

Data Recipient		**Date of Audit**	dd – dd mmm yyyy
Named Contact		**NHS Digital Audit Team**	< Lead Auditor > < Auditor > < SME >
Location(s) of Audit			
Scope of Audit	Type of audit: < see Audit Guide section 2.3 > Data Sharing Framework Contract: < reference > Data Sharing Agreement(s): < reference(s) > < any special information >		

Audit Plan	Focus	Names and role of attendees
[Date]		
9:30 – 9:40	Opening meeting	*Please list names and roles***
9:40 – 10:00	Background to organisation and data sharing agreement	*Please list names and roles***
10:00 – 12:30	Information transfer Access control	*Please list names and roles***
12:30 – 13:15	Auditor time and lunch	
13.15 – 15.45	Use and benefit of data Operational planning and control	*Please list names and roles***
15:45 – 16:15	Auditor time	
16:15 – 16:30	Feedback on the day and any changes in the schedule for tomorrow	*Please list names and roles***
[Date]		
9:30 – 12:15	Risk assessment and treatment Destruction of data Where appropriate and time allows, the Audit Team will visit the location where NHS Digital data is located / held.	*Please list names and roles***
12.15 – 13:00	Auditor time and lunch	
13:00 – 14.30	Outstanding issues Opportunity to provide evidence that was not available at the time of meeting.	
14:30 – 15:30	Auditor time	
15:30 – 16:15	Closing meeting	*Please list names and roles***

** To be populated with list of names and roles for persons attending on behalf of the organisation to answer questions round the topics area. Expected attendance is between 1 and 4 people, except for opening and closing meetings.

Appendix C Data Sharing Audit - Action Plan

The following table shows a representative action plan which a data recipient may use to record the actions to address the audit findings, see section 2.14. This table is available as an independent download from the NHS Digital website: http://digital.nhs.uk/dsa.

The four status assignments are:

- Open – the action is still be progressed;
- Closed – the action has been suitably completed;
- On hold – the action has been suspended temporarily; and
- Rejected – the data recipient has chosen not to action an Observation raised by the Audit Team. A brief statement should be included under "Action Proposed / Taken" as to why the observation was rejected.

Ref	NHS Digital Finding	Designation	Action Proposed / Taken	Owner	Due Date	Status
1.		Select			Select	Select
2.		Select			Select	Select
3.		Select			Select	Select
4.		Select			Select	Select
5.		Select			Select	Select
6.		Select			Select	Select
7.		Select			Select	Select
8.		Select			Select	Select