

Data Sharing Audits: A Guide for Data Recipients

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

Version 2.2

Published May 2018



**Information and technology
for better health and care**

Contents

1	Introduction	3
1.1	Why is NHS Digital conducting data sharing audits?	3
1.2	Who is this guide for?	3
2	The Data Sharing Audit Process	3
2.1	The Audit Team	3
2.2	How is an organisation selected for audit?	4
2.3	Types of data sharing audits	4
2.4	Scope of a data sharing audit	5
2.5	Informing an organisation of an audit	5
2.6	What material will the Audit Team want to see?	6
2.7	The onsite visit	7
2.8	Nonconformities and observations definitions	8
2.9	Risk Statement	9
2.10	Draft and final reports	10
2.11	Publication	10
2.12	NHS Digital action resulting from an audit	11
2.13	Data recipient response to findings	11
2.14	Timescales	11
2.15	Post audit review	12
2.16	The data recipient experiences an issue	13
2.17	Providing feedback	13
Appendix A	Examples of Evidence	14
Appendix B	Representative NHS Digital Audit Plan	18
Appendix C	Data Sharing Audit - Action Plan	20

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.

This version of the Audit Guide has been developed to incorporate feedback from data recipients and NHS Digital teams received over the previous year.

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 suitably experienced and hold relevant international and/or industry recognised qualifications.

For certain audits, the Audit Team may include Subject Matter Experts from other teams within NHS Digital to ensure the necessary balance of expertise and competence.

2.2 How is an organisation selected for audit?

A data recipient can be selected to be audited by teams responsible for the release of data within NHS Digital:

- prior to the receipt of data (to seek confidence in an organisation's ability to handle data securely);
- whilst in the possession of NHS Digital data; or
- following destruction of the supplied data.

A data recipient is not expected to be audited more than once during the life of a specific data sharing agreement, 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; or
- an organisation has many different data sharing agreements for different datasets or extracts of data and therefore there is a risk of linking / identification.

2.3 Types of data sharing audits

A data sharing audit will fall under one of the following four 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.
2. **Focused** - This audit is similar to a routine audit but will focus on specific elements (for example, data destruction). Due to the tighter scope, the onsite visit will generally be shorter than for a routine audit.
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 topics listed in section 2.4 except for Use and Benefits as a pre-release audit will be conducted prior to these being available.
4. **Heightened concern** - This audit will be conducted on a data recipient that has been subject to scrutiny by NHS Digital. This scrutiny may result following an incident and suspension of access to data. In certain circumstances the audit will be unannounced. The scope of the audit will be dependent on the nature of the concern raised.

The reporting process will be the same for all audits, see section 2.10.

Depending on the nature of the findings identified, a post audit review may be conducted, see section 2.15.

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 data recipient along with its associated documentation. The ready availability of suitable evidence will play a key part in the audit.

An audit is also likely to involve any data processor engaged by the data recipient to ensure that a complete understanding of the handling of the data is obtained.

Fundamentally, the audit will seek to determine whether:

- the data recipient is adhering to, or could adhere to, the requirements of a data sharing framework contract and a data sharing agreement(s);
- the data handling activities performed by the data recipient pose an unacceptable risk to confidentiality or to NHS Digital; and
- the data recipient conforms to its own policies, processes and procedures.

The above criteria will also apply to any data processor engaged by the data recipient.

The six 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 selected 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 heightened concern 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 with the notification letter. This plan will be tailored by the Lead Auditor to meet the specific scope of an audit. The data recipient is expected to review the draft audit plan and identify those personnel that will attend each of the defined sessions.

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, processes 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 or concerns about the data recipient.

2.6 What material will the Audit Team want to see?

In the notification letter, the data recipient is asked to provide the policies, processes and procedures that cover the scope of the audit in advance of the onsite visit. Representative policies 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 the Data Sharing Audit report.

Material supplied by the data recipient will be retained in accordance with NHS Digital's records management retention schedule.

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.

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 data recipient has. 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. 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 physical controls.

The Audit Team will require access to relevant operational staff, including representatives from the data recipient's data processor where applicable, to understand how data supplied by NHS Digital is processed.

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, processes or procedures not supplied prior to the audit visit may also be requested by the Audit Team. Any documentation that is taken away will be handled appropriately by the Audit Team, 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 and points for follow-up.

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, except where the Lead Auditor specifies a different timeframe during the closing meeting. Therefore, findings may change as a result of the review of that evidence. There could also be occasions where issues come to attention of the Audit Team after the onsite visit these may be included in the audit report. The Lead Auditor will inform the data recipient 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 within the stipulated timeframe 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.

Prior to the publication of the draft audit report the Audit Team may seek advice from the data release team with respect to points arising from the onsite visit with regards to special constraints or agreements not expressed explicitly in the material the Audit Team had at the start of the on-site visit.

2.8 Nonconformities and observations definitions

A finding will be classified according to one of the following designations:

- Agreement nonconformity;
- Organisation nonconformity; or
- Observation.

2.8.1 Agreement nonconformity

An agreement nonconformity is failure to implement a requirement contained within a data sharing framework contract or data sharing agreement or any standard, document or guideline explicitly referenced in the data sharing framework contract.

An agreement nonconformity may be raised against guidance documentation explicitly identified within the data sharing framework contract, including later versions, except when the data recipient is able to provide a documented justification as to why such guidance is not applicable.

2.8.2 Organisation nonconformity

An organisation nonconformity is a deviation from a requirement specified in the data recipient's own policies, processes and procedures.

2.8.3 Observation

An observation may be:

- where a nonconformity has not arisen at the time of the audit, but the data recipient could fail to meet a requirement if suitable steps are not implemented in the necessary time frame. For example, the data recipient has identified members of staff that will process NHS Digital data shortly, but these staff have not completed the information governance training at the time of the audit. The observation would be for staff to complete the training prior to undertaking any processing of data; or
- a possible improvement, for example, sharing of good practice seen by the Audit Team in other data sharing audits.

2.9 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 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 controls and their correct implementation; and
- the context in which the data is being used.

The risk will be expressed as:

Critical Risk
High Risk
Medium Risk
Low Risk

2.10 Draft and final reports

A draft audit report will be issued to the data recipient within the timescale stated in Table 2. 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 after the onsite visit within the agreed timeframe (see section 2.7).

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 plus commercially confidential and security sensitive 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 timescale shown in Table 2.

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

All factual inaccuracies will be amended by the Audit Team. Other comments will be considered by the Audit Team on a case by case basis. 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 2.16.

By its very nature, a two-day audit of a data recipient processing data cannot be deemed to be conclusive. Final report findings should always be viewed in this context.

Once the report has been finalised it shall be emailed to the data recipient by the Lead Auditor along with an indicative date of when the report is to be published online. If the report identifies nonconformities the email will include a statement of when any post audit review is expected to be performed, see section 2.15. The data recipient will also be requested to supply an action plan to address all the findings, within the timescales specified in Table 2.

2.11 Publication

The data sharing audit report will be published on the external NHS Digital website. Audit reports are scheduled to be published according to the timescales specified in Table 2. Circumstances that may restrict publication include purdah and public holidays.

The NHS Digital Communications Team may use NHS Digital's Twitter account to publicise that the audit report is available online.

The website on which reports can be accessed is: <https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

2.12 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 data release team through its breach process.

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.

2.13 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. A Word version of this template can be found on the DARS audit report SharePoint site; currently <https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

The data recipient will be required to send the action plan to the Lead Auditor no later than the timescale specified in Table 2.

2.14 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
Provision of organisation's policies, processes and procedures		At least 5 working days prior to proposed audit date
Onsite visit	Agreed audit onsite visit date	
Headline findings	Within 5 working days the Lead Auditor will send an email to key NHS Digital senior managers outlining the findings raised in the closing meeting so that any action that is required immediately can be instigated, see section 2.12	
Draft audit report issued to data recipient for comment	Within 10 working days following onsite visit	
Any comments on the draft audit report returned to Lead Auditor		Within 10 working days of receipt of draft audit report
Final audit report produced following an internal publication meeting and issued to the data recipient	The publication meeting is typically held first week of the month	
Final audit report published on NHS Digital website	Typically, the third week of the month	
Data recipient provides NHS Digital with action plan to audit report		Within 10 working days from issue of the final report to the data recipient

Table 2: Audit Timings

2.15 Post audit review

The actions taken by the data recipient to address the findings presented in the published audit report 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 or accompanying auditor will be responsible for any post audit review. A review of the data recipient's action plan and suitable supporting evidence to demonstrate the action addresses the finding and is suitably effective will be undertaken.

NHS Digital will contact the organisation, usually by email, to request an update on progress of the action plan. A post audit review will generally be conducted three to four months following publication of the audit report. However, the timing will depend on the criticality of any of the findings and any action taken by the NHS Digital data release team (see section 2.12). The actual timing of a post audit review will be communicated to the data recipient by the Lead Auditor when issuing the final report.

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.

The Lead Auditor will highlight internally any serious concerns in relation to any nonconformities which have not been addressed or the corrective action taken itself represents a serious risk to NHS Digital, see section 2.12.

A draft post audit review report will be written following the review. The report will be produced in the same way as the audit report and will detail progress taken to address the findings raised. The risk statement will be updated accordingly.

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

2.16 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:

<https://www.digital.nhs.uk/feedback-complaints>

2.17 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 final audit report has been released.

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
<ul style="list-style-type: none"> 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 third-parties? Are technical reviews carried out when platforms are changed? 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> • 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 security testing, for example penetration testing and vulnerability assessments, undertaken by the organisation? • Does the organisation have policies, processes and procedures related to patch management? 	<ul style="list-style-type: none"> • 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 • Security assessments, including external and internal penetration tests

Use and benefits of data	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • Publications and research papers • Analytical software / tools • Sub-licencing arrangements • Operating procedures

Data destruction	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • Is there an established framework for the destruction of data and the media on which data is recorded (paper and electronic)? • Does the organisation maintain sufficiently detailed records for those items sent for destruction? • Are decommissioned assets held in a secure area until destroyed? • How are assets destroyed? • Is a suitable third party used to destroy assets? What records are produced by the third-party to demonstrate that the assets have been destroyed? • How is the destruction of an asset linked back to the equipment asset register? • Have Data Destruction Certificate(s) been returned to NHS Digital? 	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Does the organisation have a formal risk and issue management process? • Are risks to data assets, including those associated with the technical infrastructure, assessed to ensure that data is secure? • Does the organisation have a declared risk appetite? • 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? 	<ul style="list-style-type: none"> • Risk management framework / procedure • Risk register(s) and associated controls • Risk assessments / mitigation • Privacy impact assessments • Minutes of management meetings • Risk assurance reports to Senior Management

Operational management and control	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • How does the organisation remain compliant with legal and contractual requirements? • What are the organisation's information security and information governance assurance processes? • Who has responsibility to manage and control information governance processes? • How are new and updated policies/processes/procedures communicated to all staff? • Does the organisation have an internal audit programme in place? • 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/processes/procedures related to configuration control and asset management in place? • Does the organisation have an established information governance training programme, which includes refresher training? 	<ul style="list-style-type: none"> • Information Security Policy and Information Governance Framework • Information governance policies • Evidence of Senior Management ownership of information governance • Minutes of meetings • Change management processes and any associated tools • Policies, processes, procedures and tools related to configuration control, 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 • 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 >
Location(s) of Audit			< Auditor > < SME >
Scope of Audit	Type of audit: < Routine / Focused / Pre-release / Heightened Concern > Data Sharing Framework Contract: < reference > Data Sharing Agreement(s): < reference(s) > < any special information >		

Audit Plan	Focus	Names and role of attendees
[Date]		
9:00 – 9:30	Auditor preparation time	Not required
9:30 – 9:40	Opening meeting	<i>Please list names and roles**</i>
9:40 – 10:00	Background to organisation and data sharing agreement	<i>Please list names and roles**</i>
10:00 – 12:30	Information transfer Access control	<i>Please list names and roles**</i>
12:30 – 13:30	Auditor time and lunch	Not required
13.30 – 16:00	Data destruction Operational management and control	<i>Please list names and roles**</i>
16:00 – 16:20	Auditor time	Not required
16:20 – 16:30	Feedback on any changes in the schedule for day 2. Please note that no feedback on findings will be given at this stage.	<i>Main contact or delegate</i>
[Date]		
9:00 – 9:30	Auditor preparation time	Not required
9:30 – 12:15	Use and benefits of data Risk management Where appropriate and time allows, the Audit Team will visit the location where NHS Digital data is located / held.	<i>Please list names and roles**</i>
12.15 – 13:00	Auditor time and lunch	Not required
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	Not required
15:30 – 16:15	Closing meeting	<i>Please list names and roles**</i>

** 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 2.13. This table is available as an independent download from the NHS Digital website: <https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

The four status assignments are:

- Open – the action is still being 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