

Data Sharing Audits: A Guide for Data Recipients

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



Contents

1	Introduction	3
1.1	Why is NHS England 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	Selecting a data recipient for audit	4
2.3	Types of data sharing audits	4
2.4	Audit scope	4
2.5	Notifying a data recipient of an audit	5
2.6	Introductory telephone call	5
2.7	Representatives required at the audit interviews	5
2.8	Documents the Audit Team will want to see	6
2.9	Data processing statement	7
2.10	Audit Interviews	7
2.11	Definition of findings	8
2.12	Risk Statement	9
2.13	Draft report	10
2.14	Headline findings to NHS England	10
2.15	NHS England Publication Meeting	10
2.16	Final Report and Action Plan template	11
2.17	Publication on Internet	11
2.18	NHS England action resulting from an audit	11
2.19	Data recipient response to findings	11
2.20	Timescales	11
2.21	Post audit review	12
2.22	Issues and concerns	13
2.23	Providing feedback	13
Appendix A	Examples of Evidence	14
Appendix B	Audit Plan	17
Appendix C	Documentation Checklist	20
Appendix D	Action Plan	24
Appendix E	Glossary	25

1 Introduction

1.1 Why is NHS England conducting data sharing audits?

NHS England has a legal duty to maintain the confidentiality, safety, security and integrity of all personal and patient data it holds and disseminates. This duty is defined through the Health and Social Care Act 2022, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and common law duty of confidentiality.

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

NHS England audits data recipients 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 England under a DSFC and a DSA for the purposes of benefitting health and social care. This guide is designed to provide an overview of NHS England's management of the data sharing audit process so that:

- data recipients understand how the NHS England Audit Team will approach an audit
- there is enhanced public trust in one of the ways in which NHS England assures the release of data provided to organisations.

Within the context of this guide the term “data recipient” also encompasses any processors or third parties engaged as part of a DSA. This will also include undeclared parties in the DSA that also receive the data.

2 The Data Sharing Audit Process

This section guides the data recipient through each stage of a data sharing audit, though in certain instances some stages may not apply. An audit may be undertaken:

- remotely
- on-site.

Differences between audits conducted on-site or remotely will be explicitly described in this guide.

2.1 The Audit Team

NHS England has established an independent audit function that is separate from the Data Access Request Service (DARS).

Audit Team personnel are suitably experienced and hold relevant international and/or industry recognised auditing and technical qualifications.

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

2.2 Selecting a data recipient for audit

A data recipient can be selected for audit by DARS:

- to seek confidence in its ability to handle data securely prior to the receipt of data
- whilst in the possession of data supplied by NHS England or granted access to data held in NHS England's Data Access Environment (DAE)
- following destruction of the supplied data.

The Audit Team is then commissioned by DARS to audit the selected data recipient.

The Audit Team may also independently identify a data recipient from available data dissemination lists. Such audits would be confirmed with DARS and follow the same process described below.

2.3 Types of data sharing audits

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

1. **Routine** - audit of a data recipient already in receipt of data which will look at the full range of topics listed in section 2.4.
2. **Focused** - audit that concentrates on specific elements, for example, data destruction. The overall duration of the audit interviews will generally be shorter than for a routine audit. A focussed audit will also apply to those organisations accessing the DAE.
3. **Pre-release** - audit prior to any release to ensure that the data recipient can handle data appropriately. This type of audit will normally consider the topics listed in section 2.4 except for use and benefits of data.
4. **Heightened concern** - audit to consider concerns raised within NHS England. The scope of the audit will be dependent on the nature of the concern raised.

The type of audit will be declared in the notification letter and in the audit plan.

The reporting process described later in this document will be the same for all audits.

2.4 Audit scope

The audit scope will cover the data recipient's management and use of data provided by NHS England.

The six scope areas usually considered by the Audit Team are:

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

The Audit Team will advise the data recipient when the scope deviates from the above.

The audit will seek to determine whether:

- the data recipient is adhering to, or could adhere to, the requirements of the DSFC and DSA(s). An example contract and agreement can be found at <https://digital.nhs.uk/services/data-access-request-service-dars>
- the data handling activities performed by the data recipient pose an unacceptable risk to confidentiality or to NHS England
- the data recipient conforms to its own policies, processes and procedures.

An audit may also involve any processor or third party engaged by the data recipient to ensure that a complete understanding of the handling of the supplied data is obtained. The above checks will also apply to such parties.

Typical opening questions and types of evidence required related to the six scope areas are detailed in Appendix A.

2.5 Notifying a data recipient of an audit

Once a data recipient has been selected for an audit, the Audit Team will send a notification letter to the data recipient's main contact. This letter will be sent by email no less than 10 working days prior to the proposed audit date.

In exceptional circumstances the data recipient may seek an alternative date for the audit, which must be raised prior to the telephone call with the Audit Team, see section 2.6.

The Audit Team will provide a draft audit plan (Appendix B) and a document checklist (Appendix C) with the notification letter. The draft audit plan will meet the specific scope of the audit. The data recipient will review the draft audit plan and identify the names of personnel that will attend each session.

2.6 Introductory telephone call

Following receipt of the notification letter, the Lead Auditor will arrange a call with the data recipient to discuss:

- the audit process
- any requested changes to the audit date
- the audit plan and who should attend from the data recipient and from any supporting organisation, for example, joint Controllers, Processors and third parties (see section 2.7)
- logistics for audit interviews
- documentation to be supplied by the data recipient prior to the audit interviews (see section 2.8)
- any requirement to visit a data centre or third parties on-site.

2.7 Representatives required at the audit interviews

The Audit Team will require access to managerial, operational and technical personnel who are able to cover the areas detailed in the scope and understand how data supplied by NHS England is processed.

The following table gives an overview of the key staff likely to be involved for each of the defined scope areas. The actual staff involved will depend on the roles and responsibilities they undertake in the organisation. Further representation may also be needed from third parties including processors. It is essential that staff are present during the audit interviews who can answer the type of questions and provide the types of evidence detailed in Appendix A.

Scope Area	Typical representation
Use and Benefits	Business Intelligence Staff involved in processing data / producing outputs, for example, researchers and analysts
Information Transfer	Business Intelligence Staff involved in processing the data, for example, researchers and analysts Information Security Information Technology
Access Control	Information Security Information Technology
Data Destruction	Information Security Information Technology
Operational Management and Control	Information Governance Human Resources
Risk Management	Risk Management

Table 1: Key representatives for the audit interviews

The Audit Team may also request a tour of the locations where data supplied by NHS England is being processed and stored. This tour may be done virtually for remote audits. For on-site audits, the data recipient will need to make available personnel to escort the Audit Team.

If the data recipient is unsure which representatives are required or appropriate, this can be discussed during the telephone call with the Lead Auditor, see section 2.6.

2.8 Documents the Audit Team will want to see

Prior to the audit interviews, relevant documentation will be submitted to the Audit Team. A document checklist, Appendix C, will be provided with the notification letter for completion by the data recipient. As document names and content vary across organisations, it is the responsibility of the data recipient to indicate titles on the document checklist and supply the relevant material.

These documents will be used to supplement and inform the audit and will be reviewed by the Audit Team prior to the audit interviews. The notification letter will specify the date by which documentation is to be provided. A finding may be included in the audit report when documents are not provided prior to the audit interviews without a reasonable justification.

2.9 Data processing statement

The personal data the Audit Team holds about a data recipient includes personal data provided to NHS England as part of the data application process in support of audit activities and on completed feedback questionnaires. This personal data will only be used for administrative and audit delivery purposes; it will not be supplied to any other party outside of the data sharing audit function. It may, however, be shared with an external audit organisation commissioned by NHS England to undertake audits on behalf of the data sharing Audit Team.

The Audit Team maintains an audit database which holds contact information and key milestone dates. Access to the database is limited to staff within the NHS England audit function.

All documentation supplied by, or on behalf of, a data recipient will be held securely by NHS England. Access is limited to the data sharing audit team, its support personnel and management team.

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

For more details around how NHS England uses personal data, in line with the UK GDPR, see [NHS England as a data controller](#)

NHS England may receive requests under the Freedom of Information Act 2000 to disclose information in relation to an audit. Requests for information are looked at on a case-by-case basis by the appropriate team within NHS England. The team responsible for freedom of information requests may consult with the data recipient in question before responding to the request.

2.10 Audit Interviews

Audits interviews are spread across a number of days and will usually involve 2 auditors from NHS England. The actual number of days and team members will be shown in the audit plan sent with the notification letter. The Audit Team will try to keep disruption to the data recipient to a minimum through the agreement of the audit plan. Where the third party is different from the data recipient, the need to organise separate meetings will be identified at the audit planning stage.

If the interviews are being conducted on-site, then the data recipient shall provide a dedicated room, at each location identified in the audit plan, for the Audit Team to conduct interviews and review documentation / evidence. The Audit Team may also need to conduct information reviews or equipment checks in different areas of the facility. Internet access will be requested in advance, if required.

2.10.1 Opening meeting

The Audit Team will hold an opening meeting with representatives from the data recipient to explain the audit process. The meeting will provide an opportunity to discuss any issues or concerns with respect to the audit process. The Audit Team may make minor changes to the audit plan timings at the opening meeting should the need arise.

2.10.2 Audit interviews and reviews

Interviews will be broken down into short sessions. These sessions will focus on a specific area of the audit scope and kept at a length to ensure participant comfort. Where the audit is done remotely, the Microsoft Teams sessions will not be recorded nor will screenshots be taken by the Audit Team.

Additional sessions may be scheduled by the Audit Team if there is a need to speak to other staff or if there is a need to explore the area further.

The Audit Team will conduct an evidence-based assessment of the data recipient's controls and environment where data supplied by NHS England resides. The Audit Team will undertake interviews of relevant staff, review documents, records and uses of data along with an inspection of implemented controls.

The questions asked by the Audit Team and evidence gathered will relate to the audit scope. There are some generic areas which are normally covered during an audit, examples of these areas are detailed in Appendix A.

The most important elements of an audit are timely access to supporting evidence and to appropriate staff who answer questions openly, comprehensively and accurately.

The Audit Team will make and retain notes from interviews, observations and testing. Further documentation or evidence may be requested for review by the Audit Team. Such documents will be handled appropriately, as outlined in section 2.9.

2.10.3 Closing meeting

The Audit Team will hold a closing meeting with the data recipient's representatives to discuss the identified findings. The findings will be caveated if pre-existing material still needs to be provided by the data recipient.

2.10.4 Identification of findings

The Auditor Team may conduct a further review of its notes after the closing meeting, which could identify new findings. New findings will be communicated to the data recipient and included in the draft audit report.

Any finding identified during the audit and corrected by the data recipient prior to the closing meeting will be recorded in the audit report together with an acknowledgement that the issue was corrected.

The Audit Team may request pre-existing evidence that was unavailable during audit interviews to be supplied within five working days after the closing meeting, except where the Lead Auditor specifies a different timeframe during the closing meeting.

The Audit Team will not review new material generated after the opening meeting or existing material updated after the closing meeting; such material may be reviewed as part of a post audit review (see section 2.21).

If any issues of a serious nature are identified during the audit, then the Audit Team will raise its concerns with the data recipient and NHS England immediately.

2.11 Definition of findings

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

- Agreement nonconformity
- Organisation nonconformity

- Observation
- Opportunity for improvement
- Follow-up.

2.11.1 Agreement nonconformity

An agreement nonconformity is a failure to implement a requirement contained in a DSFC or DSA, or in a communication (for example, letter or email) between NHS England and the data recipient during or after the application.

An agreement nonconformity may also be raised against guidelines identified in the DSFC, except when the data recipient is able to provide a documented justification (and agreed with NHS England in writing) as to why such guidance is not applicable.

2.11.2 Organisation nonconformity

An organisation nonconformity is a deviation from a requirement specified in the data recipient's own documentation.

2.11.3 Observation

An observation is a situation where a nonconformity had not arisen at the time of the audit but without appropriate action being taken a nonconformity could result. For example, the data recipient has identified members of staff that will process data supplied by NHS England shortly, but those staff have not completed the information governance training at the time of the audit. The observation would be that staff need to complete the training prior to processing data.

2.11.4 Opportunity for improvement

The Audit Team may identify opportunities for improvement which could help an organisation improve its controls or their effectiveness based on the Audit Team's experience and knowledge from other data sharing audits.

2.11.5 Follow-up

Any material considered important by the Audit Team that could not be provided within the stipulated timeframe or in the case of a remote audit could only be confirmed onsite by the Audit Team, may be identified in the audit report as a point for follow-up. This material will be reviewed, by the Audit Team, at the post audit review. If issues are identified during the post audit review, further findings may be raised by the Audit Team.

2.12 Risk Statement

The Audit Team will provide an overall risk statement in the audit report 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 which could cause harm or distress
- the soundness of the data recipient's controls and their correct implementation
- the context in which the data is being used.

The risk will be expressed as:

- Critical Risk
- High Risk
- Medium Risk
- Low Risk

2.13 Draft report

The Audit Team will issue a draft audit report to the data recipient within the timescale stated in Table 2 (see section 2.20). The report will detail findings as described at the closing meeting and, if relevant, amended following the review of any documentation provided to the Audit Team after the closing meeting.

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 compliance checks described in section 2.4. The audit report may 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 and for commercially confidential and security sensitive information. 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 the draft audit report has been accepted as factually accurate. If a data recipient requires additional time to consider its response, an extension request must be sent to the Lead Auditor using the email address given in the notification letter within the stated timeframe.

All factual inaccuracies will be corrected by the Audit Team. Other comments will be considered by the Audit Team on a case-by-case basis. Although rare, disagreement concerning the findings may occur between the two parties. Whilst it is a matter for the Audit Team to determine the content of the final report, where there is a non-resolvable disagreement, a comment will be added to the report to reflect the data recipient's opinion. See also section 2.22.

The audit is based upon a sample of the data recipient's activities, as observed by the Audit Team. Therefore, the findings detailed in the audit report may not include all possible nonconformities which may exist.

2.14 Headline findings to NHS England

A headline findings email will be issued to senior managers in NHS England by the Audit Team within the timescale stated in Table 2. The email will present the nonconformities, observations, opportunities for improvement, points for follow up and any other matters of interest which may be material to the audit.

2.15 NHS England Publication Meeting

Following the receipt of comments from the data recipient, the Audit Team will make any changes to the draft report which is then taken to the next internal publication meeting. This meeting is attended by the Audit Team and representatives from DARS and Communications. The purpose of the meeting is to provide an opportunity for other specialist teams within NHS England to offer advice and commentary on the draft audit report prior to its publication.

If any material changes to the report are suggested at the meeting and accepted by the Audit Team, then the Lead Auditor will discuss the changes with the data recipient prior to publication.

2.16 Final Report and Action Plan template

The Lead Auditor will email the final audit report to the data recipient and provide an indication of when the report is to be published online.

If the final audit report contains nonconformities, observations or items for follow-up, the email will state when a post audit review is expected to be performed, see section 2.21. The data recipient will also be requested to complete an action plan which address all the findings, see section 2.19.

2.17 Publication on Internet

The data sharing audit report will be published by the Audit Team on the external NHS England website: <https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

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.

2.18 NHS England action resulting from an audit

Findings that present a serious divergence from the contract or agreement, or those findings which present an unacceptable risk to NHS England or to its stakeholders (including patients), will be addressed directly by DARS through its breach process.

A decision will be made by the NHS England Senior Information Risk Owner (SIRO), or representative, or the Service Director for Data Dissemination on the course of action to take in response to any identified nonconformities.

2.19 Data recipient response to findings

The audit report may require a data recipient to provide an action plan which details the action to be taken, the name of the action owner and the target date for each action. It is the responsibility of the data recipient to decide on an appropriate course of action and ensure it addresses the finding.

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 D. A Word version of this template can be found on the data sharing audit website: <https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

The data recipient will send the annotated action plan to the Lead Auditor no later than the timescale specified in Table 2. The Audit Team will review the action plan and check that the actions planned by the data recipient have the potential to address the findings and the timescales appear reasonable. The Lead Auditor will inform the data recipient of any concerns with respect to the proposed action plan.

2.20 Timescales

The timescales shown in Table 2 will be dependent upon the outcomes of the audit and are subject to change.

Action	Responsibility of NHS England	Responsibility of data recipient
Send out notification letter and draft audit plan	Minimum of 10 working days prior to proposed audit interviews	
Completed audit plan returned to the Lead Auditor		As defined in the notification letter, but a minimum of 5 working days prior to proposed audit interviews
Provision of data recipient's documentation		As defined in the notification letter, but a minimum of 5 working days prior to proposed audit interviews
Audit interviews	Agreed dates	
Headline findings to NHS England Senior Managers	Within 5 working days of the closing meeting	
Draft audit report issued to data recipient for comment	Within 10 working days following the closing meeting	
Any comments on the draft audit report returned to Lead Auditor		Within 10 working days of receipt of draft audit report
Internal publication meeting	The publication meeting is typically held first week of the month	
Final audit report produced and sent to the data recipient	At least 5 working days prior to the report being published on the NHS England website	
Final audit report published on NHS England website	Typically, the third week of the month	
Provide annotated action plan		Within 10 working days from issue of the final report to the data recipient

Table 2: Audit Timings

2.21 Post audit review

The Audit Team will assess the actions taken by the data recipient to address the findings presented in the published audit report as part of a post audit review.

A review of the data recipient's action plan and supporting evidence to demonstrate the actions address the findings and are effective will be undertaken by a member of the Audit Team.

The Audit Team will contact the data recipient to request an update on progress of the action plan. A post audit review will generally be conducted 3 to 6 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 NHS England (see section 2.18). The actual timing of a post audit review will be communicated to the data recipient by the Lead Auditor with the final report.

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

The review will comprise at least one of the following:

- independent desktop review of the evidence
- telephone / conference call to walk through the evidence
- video call so that evidence held on the data recipient's system can be presented
- an onsite visit.

The Audit Team will raise 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 England, see section 2.18.

A draft post audit review report will be written following the review. The report will be produced in the same way as the original 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.

2.22 Issues and concerns

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

The NHS England complaints procedure can be found at:
[NHS England » Complaining to NHS England](#)

2.23 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 a link to a feedback questionnaire once the final data sharing audit report has been released by the Audit Team.

All feedback will be reviewed and any unsatisfactory score may be followed up to improve our services.

Appendix A Examples of Evidence

This appendix describes the type of questions and typical evidence for each 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 with 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 and are effective.

The following tables provide examples of evidence 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 data recipient will only be required to supply this once.

Use and benefits of data	
Aim: Determine the data is being used for the agreed purpose and that suitable checks are made prior to any release / publication	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • Is the data being used in accordance with the agreed purpose? • Are the declared benefits being achieved? • Has the data recipient recognised NHS England's copyright, when appropriate? 	<ul style="list-style-type: none"> • Publications and research papers • Analytical software / tools • Sub-licencing arrangements • Operating procedures • Output register of deliverables / research papers

Information transfer	
Aim: Establish the flow of data supplied by NHS England and the infrastructure being used to process and store such data, identifying all data touchpoints	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • Describe the data recipient'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 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 and 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 • Storage and backup policies • Data in-transit encryption algorithms • Contract/agreements with any processors or third-party data centres involved in processing or storing data supplied by NHS England • Sub-licencing arrangements

Access control	
Aim: Establish the controls and security measures in place at the processing and storage locations to control access to the data	
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 data recipient? • Does the data recipient have policies, processes and procedures related to asset management patch management, configuration control in place? • How does the data recipient ensure any information passing over public networks is protected from fraudulent use, modification or disclosure? 	<ul style="list-style-type: none"> • Information security policies and guidance • Account protection including organisational IT infrastructure, for example, firewalls, encryption, anti-virus / anti-malware and patching • User / customer access permissions • Authentication process including logging and monitoring • Hardware and mobile device user management • Hardware and software encryption • Joiners, leavers and movers processes • Change management process • Password policy and processes • Physical building access controls • Remote access policy • Guest access policy • Physical and environment controls around the storage of data (server rooms and data centre) • Security assessments, including vulnerability assessment and penetration tests reports

Data destruction	
Aim: Determine whether the data is adequately destroyed electronically or physically from all established touch points	
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 data recipient 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 Certificate(s) of Destruction been returned to NHS England? 	<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 • Certificates of destruction sent to NHS England • Destruction of paper-based information records

Operational management and control	
Aim: Assess the data recipient's internal controls to ensure that data is handled appropriately and that these controls are known to relevant staff and have been independently validated	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • How does the data recipient remain compliant with legal and contractual requirements? • What are the data recipient'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 data recipient have an internal audit programme in place? • How does the data recipient identify and manage its information and equipment assets? • How does the data recipient manage and report incidents? • Does the data recipient have an established information governance training programme, which includes refresher training? 	<ul style="list-style-type: none"> • Information Governance Framework • Information Governance policies • Data Protection Impact Assessment • Evidence of Senior Management ownership of information governance • Terms of Reference for governance bodies • Minutes of meetings / action logs • Incident management processes and any associated tools / incident reports • Information asset register • Record of Processing Activity • 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

Risk management	
Aim: Ensure risks around the handling of the data have been identified, documented and, where necessary, mitigated	
Typical opening questions/requests	Examples of evidence
<ul style="list-style-type: none"> • Does the data recipient have a formal risk and issue management process? • Have IT, IG and project risks associated with the NHS England data assets been identified and recorded? • Does the data recipient 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 • Terms of Reference for risk committee • Minutes of management meetings • Risk assurance reports to Senior Management

Appendix B Audit Plan

Based on the audit scope (see section 2.4), the location of the audit (including remote) and the number of organisations involved, the Audit Team will create an audit plan to be completed by the data recipient. Normally the days on site would be consecutive.

B.1 Representative on-site audit plan

Data Recipient	<i>[Organisation]</i>	Date of Audit	<i>[Dates]</i>
Named Contact	<i>[Name]</i>	NHS England Audit Team	<i>[Names]</i>
Location(s) of Audit			
Scope of Audit	Type of audit: <i>[Type]</i> Data Sharing Framework Contract: <i>[reference]</i> Data Sharing Agreement(s): <i>[reference(s)]</i> <i>[any special information]</i>		

Audit Plan	Focus	Names and role of attendees
[Date]		
9:00 – 9:30	Audit team preparation time	NHS England auditors only
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 – 12:45	Information transfer Access control	Please list names and roles**
12:45 – 13:45	Auditor time and lunch	NHS England auditors only
13.45 – 14:45	Data destruction	Please list names and roles**
14.45 – 16:30	Operational management and control	Please list names and roles**
16:30 – 16:45	Auditor time	NHS England auditors only
16:45 – 17:00	Feedback on the day and any changes in the schedule for tomorrow	Please list names and roles**
[Date]		
9:00 – 9:30	Audit team preparation time	NHS England auditors only
9:30 – 9:45	Receipt of any available evidence	As required
9:45 – 10:30	Use and benefits of data	Please list names and roles**
10:30 – 11:15	Risk management	Please list names and roles**
11:15 – 12:00	Where appropriate and time allows, we will visit the location where NHS England data is located / held.	Please list names and roles**
12.00 – 13:00	Auditor time and lunch	NHS England auditors only
13:00 – 14.30	Opportunity to provide evidence that was not available at the time of meeting.	As required
14:30 – 15:30	Auditor time	NHS England auditors only
15:30 – 16:15	Closing meeting	Please list names and roles**

** To be populated by Auditee 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 3 people, including staff involved in day-to-day activities, except for opening and closing meetings.

B.2 Representative remote audit plan

Data Recipient	<i>[Organisation]</i>	Date of Audit	<i>[Dates]</i>
Named Contact	<i>[Name]</i>	NHS England Audit Team	<i>[Names]</i>
Conferencing Platform	Microsoft Teams		
Scope of Audit	Type of audit: <i>[Type]</i> Data Sharing Framework Contract: <i>[reference]</i> Data Sharing Agreement(s): <i>[reference(s)]</i> <i>[any special information]</i>		

Audit Plan	Focus	Names of attendees
[Date]		
10:00 – 10:30	Opening meeting including introduction to the audit Changes to the future schedule	Please list names**
10:30 – 12:00	Background to organisation and Data Sharing Agreement Use and benefits of data	Please list names**
14:00 – 15:30	Sub-licencing	Please list names**
[Date]		
10:00 – 12:30	Information transfer Access control	Please list names**
14:00 – 15:00	Data destruction	Please list names**
15:00 – 15:10	Any changes to the future schedule	Please list names**
[Date]		
10:00 – 12:00	Operational management and control	Please list names**
12:00 – 12:30	Risk management	Please list names**
12:30 – 12:40	Any changes to the future schedule	Please list names**
[Date]		
tbc	Opportunity to provide / discuss evidence that was not available at the time of meeting.	As required
[Date]		
10:00 – 11:30	Closing meeting	Please list names**

** To be populated by Auditee with list of names attending on behalf of the organisation to answer questions round the topics area. Expected attendance is between 1 and 3 people, including staff involved in day-to-day activities, except for opening and closing meetings.

Please also complete the following table with roles and email addresses. The email address is to enable the representative to be invited to the conference call.

Name of attendee	Role	Email address

Appendix C Document Checklist

This checklist indicates the type of controlled and uncontrolled documents which should be provided to the NHS England Audit Team prior to the audit interviews. Controlled documents could be strategies, policies, procedures, work instructions or guidelines. Uncontrolled documents may be lists, general organisation information or specific documents / evidence.

The Audit Team requires those documents which cover the defined scope areas. Some documents may cover several areas, or several documents may relate to a specific aspect of the audit. The list is not exhaustive and any relevant controlled documents which are applicable to the data recipient and third parties, involved in processing data, should be supplied.

The data recipient should identify in the righthand column which documents have been supplied against the referenced representative documents.

Note: please do not embed documents within this checklist. Documents are to be provided separately.

Organisation Background and Data Sharing Agreement: Key organisation aspects and people		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> Organisational and governance structure Key staff roles and responsibilities Infrastructure of ICT and IG: in-house or outsourced 	Organisation and departmental organograms	
	Governance structure including key roles and responsibilities	
	List of Information Asset Administrators (IAAs) and Information Asset Owners (IAOs) for data assets supplied by NHS England	

Use and benefits of data: Review outputs from the data and quality checks prior to use and publication		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> Tangible outputs against the Data Sharing Agreement Quality checks on outputs - copyright statement, NHS England disclosure controls 	Quality Control Policy	
	Quality committee terms of reference (or equivalent)	
	Management of datasets	
	Outputs register	
	Publication and research papers	
<ul style="list-style-type: none"> Sub-licensing arrangements (if applicable) 	The sub-licensing process	
	Sub-licensing agreement with user and organisation	
	Terms of Reference for body which approves data access requests	

Information Transfer: Assess all touch points for the data		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> • Information flow mapping • Information security • Storage and backup • Contract / agreements with data processors / third parties / sub-licencing 	Data flow diagram (to include all touchpoints of the data provided)	
	Data handling	
	Storage and backup	
	Contract / agreements with third parties providing processing, storage and deletion services (if such contracts are deemed commercially sensitive, the Audit Team will review during the interviews)	

Access control: Review the access controls in place at the storage and processing locations		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> • Account protection • Physical and environmental controls • Access permissions • Joiners, leavers and movers • Password management and authentication process • Security assessments • IT system and access change management 	Information security	
	Network security	
	Data security including encryption	
	Mobile working management	
	IT patch management	
	Password management	
	Access management and control	
	Acceptable use	
	User and administration account management	
	Anti-virus and malware	
	Logging and monitoring	
	Remote access	
	Use of removable media	
	Data storage	
	Penetration testing and vulnerability scanning	
Starters, leavers and movers		
Data centre security		

Data destruction: Data destruction and hardware disposal for each touch point		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> Data destruction - data destruction process on live system Asset disposal - hardware disposal process 	Records management	
	Data retention and disposal, including disposal of equipment assets	
	Equipment asset management lifecycle	
	Equipment Asset register	

Operational management and control: Review of IG controls, for example: owner, information asset register, incidents, training and audit, etc.		
Areas Covered	Documents Addressing	Document(s) Provided
<ul style="list-style-type: none"> Training - basic training and specialist training (IAO, IAA and Senior Information Risk Owner etc.) Information Asset Register (IAR) Policies awareness - accessibility, control, review process, communication of updates, compliance check Management and review of organisation's policies Data Protection Impact Assessment (DPIA) - review and approval process IG process covering information governance, information security, and data protection, code of conduct etc. DSPT - evidence leads, review process, independent audit Incident management Audit and compliance - audit reports, checks against contract, agreement and UK GDPR. Privacy statement and ICO registration 	Information governance	
	Management and security of information assets and information systems	
	Staff induction	
	Staff mandatory training including data protection training	
	Information / data classification	
	Records management	
	Policy and procedure management	
	Confidentiality code of practice	
	Incident management	
	DPIA covering this data	
	Record of Processing Activities (ROPA) covering this data	
	Acceptable use	
	DPIA covering this data	
	Record of Processing Activity (ROPA) covering this data	
	Terms of Reference for Governance committee(s)	

Risk management: Review of approach to managing risks and issues		
Areas Covered	Documents Addressing	Document(s) Provided
• Risk management	Risk management	
	Risk assessment template form	
	Risk management committee terms of reference (or equivalent)	
	Risk Registers (IG, IT and project / study specific)	

Appendix D Action Plan

The following table shows an action plan which a data recipient may use to record the actions proposed or taken to address the audit findings, see section 2.19. This table is available as an independent download from the following website:

<https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits>.

The three status assignments are:

- Open – the action is still being progressed
- Closed – the action has been suitably completed
- Rejected – the data recipient has chosen not to action an Opportunity for Improvement (OFI) raised by the Audit Team. A brief statement should be included under “Action Proposed / Taken” as to why the OFI was rejected

Ref	NHS England 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
9.		Select			Select	Select
10.		Select			Select	Select

Appendix E Glossary

Term	Abb	Definition
Certificate of Destruction		A certificate signed by an authorised representative of the data recipient, or specialist third party engaged to securely destroy the data and provided to NHS England within a defined timescale. The certificate assures NHS England that the data and all hard and soft copies thereof have been securely and permanently destroyed in accordance with applicable Law and guidance. The Data Destruction Certificate form can currently be download from the following webpage: Data Access Request Service (DARS): guidance notes on security – NHS Digital
Controller		Defined in Article 4 of GDPR as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”
Data		The health or social care data provided by NHS England to the data recipient under a data sharing agreement
Data Access Environment (or Trusted Research Environment)	DAE	The environment hosted by NHS England which provides secure access to the data and reduces the need for it to leave NHS England. The DAE contains a range of built-in tools to interrogate, analyse and visualise data for a more complete picture of health and care for research and planning
Data Access Request Service	DARS	Department within NHS England responsible for data sharing framework contracts, data sharing agreements and the dissemination of data
Data Protection Act	DPA	The Data Protection Act 2018 makes provision for the regulation of the processing of information relating to individuals and is the UK’s implementation of GDPR
Data Protection Impact Assessment	DPIA	A process designed to help identify and minimise the data protection risks of a project
Data Recipient		The party named in Clause 1.2 of Part 1 of the data sharing framework contract who will be a Controller of any personal data to be shared in accordance with the contract and any data sharing agreement. Within this guide, the term also includes third parties such as a Processor, sub-licensee, contractor, etc.
Data Sharing Agreement	DSA	An agreement, which sits below a data sharing framework contract, that defines the actual data to be released and the purpose for which the data has been provided
Data Sharing Framework Contract	DSFC	Overarching contract with an organisation to facilitate the sharing of data
Data Security and Protection Toolkit	DSPT	An online self-assessment toolkit managed by NHS England that enables organisations to measure and publish their performance against the National Data Guardian’s ten data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance they are practising good data security and that personal information is handled correctly

Guidance		Any applicable guidance or standards including codes of practice, standards and guidance issued by the Information Commissioner, the Department for Health, NHS England, and the Standardisation Committee for Care Information, including by way of example but not limited to those identified in Schedule 3 of the data sharing framework contract
Information Asset Administrator	IAA	Supports the IAO in fulfilling their duties, for example, ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with the IAO on incident management and ensure that information asset registers are accurate and up to date
Information Asset Owner	IAO	A senior member of staff who is the nominated owner for one or more identified information assets within the data recipient
Information Asset Register	IAR	A list of personal and non-personal information assets held by the data recipient
Information Commissioner's Office	ICO	The UK's independent body set up to uphold information rights
Information Governance	IG	Information governance is the management of information at an organisation. Information governance balances the use and security of information. Information governance helps with legal compliance and operational transparency.
Lead Auditor		The person responsible for the management of a data sharing audit on behalf of NHS England
Personal data		Defined in Article 4 of GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"
Processing		Defined in Article 4 of GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"
Processor		Defined in Article 4 of GDPR as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
Pseudonymisation		Defined in Article 4 of GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"
Senior Information Risk Owner	SIRO	Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy.
Special condition		The special conditions for processing the data as set out in the relevant data sharing agreement
Sub-licence		A written agreement between the data recipient and a sublicensee as referred to in the data sharing agreement
Touch point		A physical or logical device on which data is held, irrespective of the duration for which it is held

UK General Data Protection Regulation	UK GDPR	<p>The European Union General Data Protection Regulation, namely Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.</p> <p>The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.</p>
---------------------------------------	---------	--