Classification: Official

NHS England

Data Sharing Audits: A Guide for Data Recipients

Ensuring recipients of our data are committed to its safe handling

Contents

1. Introduction

1.1 Why is NHS England conducting data sharing audits?

NHS England (NHSE) 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 2012, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and common law duty of confidentiality.

NHSE provides information to a wide variety of organisations to support specific purposes. The purpose of a data sharing audit is to ensure that the data recipient is meeting the requirements of the Data Sharing Framework Contract (DSFC) and the Data Sharing Agreement (DSA), along with any other relevant contracts, standards and guidelines.

1.2 Who is this guide for?

This guide is designed for all data recipients with access or in receipt of data from NHSE under a DSFC, DSA and Secure Data Environment (SDE) Licencing Contract (SDE access only) for the purposes of benefitting health and social care. This guide is designed to provide an overview of NHSE's management of the data sharing audit process so that data recipients understand how the NHSE Audit Team will approach an audit.

Within the context of this guide the term "data recipient" encompasses any controllers (except NHSE), any processors or third parties engaged as part of a DSA. This will also include undeclared parties in the DSA that also receive or access the data.

There are two categories of data sharing audits that the Audit Team can carry out:

- Data dissemination – this is when an extract of the data is shared with the data recipient.
- Data access – this is when data is accessed by the data recipient through the NHSE SDE.

1.3 Audit purpose

The audit will seek to determine whether:

- The data recipient is adhering to (or could adhere to in the case of a pre-release audit) the requirements of the DSFC, DSA(s) and the SDE Licensing contract (SDE access only). An example contract and agreement can be found at https://digital.nhs.uk/services/data-access-request-service-dars.
- The data recipient conforms to its own policies, processes and procedures.

An audit may also extend to any processors or third parties engaged by the controller(s) and processor(s) to ensure a complete understanding of how the data is handled and safeguarded. The same requirements and checks will apply to these parties to confirm consistent compliance.

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

2.1 The Audit Team

NHSE has established an independent audit function that is separate from the Data Access Service (DAS).

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 to ensure the necessary balance of expertise and competence.

2.2 Selecting a data recipient for audit

An audit is commissioned by the NHSE Senior Information Risk Owner (SIRO) representative to seek confidence in the data recipient's ability to handle data securely:

- prior to the release of data
- whilst in the possession of data supplied by NHSE or accessing the data held in NHSE SDE
- following the destruction of the supplied data

The Audit Team may also independently identify a data recipient from available data dissemination lists. Such audits would be confirmed with the NHSE SIRO representative 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 types:

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.

Focused - audit that concentrates on specific elements, which could include prerelease of data. A focused audit will also apply to those organisations accessing the SDE. The overall duration of the audit interviews will generally be shorter than for a routine audit.

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 NHSE. The six scope areas considered for a routine audit are listed below:

- use and benefits of data
- information transfer
- access control

- data destruction
- operational management and control
- risk management

For a focused audit, a selection of one or more from the above topic areas would be considered.

2.5 Notification of an audit

Once a data recipient has been selected for an audit and dates agreed, the Audit Team will notify the data recipient's main contact no less than 10 working days prior to the proposed audit date to schedule the introduction call.

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 and a document checklist 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 the data shared by NHSE 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 3.

Scope Area	Typical representation
Use and Benefits	Staff involved in processing data / producing outputs, for example, principal investigator, study leads, researchers and analysts
Information Transfer	Business Intelligence Staff involved in processing the data, for example, principal investigator, study leads, 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 NHSE 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 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. If the documents are provided via a hosted platform, the Audit Team must be granted access until the audit report is finalised. The access permissions should enable the Audit Team to download and print the documents as required.

2.9 Data processing statement

The personal data the Audit Team processes about a data recipient includes information provided to NHSE as part of the data application process, in support of audit activities, and through completed feedback questionnaires. This personal data will be used solely for administrative and audit delivery purposes and will not be shared with any party outside of the data sharing audit function, unless strictly necessary.

Where required, information may be shared with an external audit supplier commissioned by NHSE to support or undertake audits on behalf of the data sharing audit team. Any such organisation will be contractually bound to process the data only for the agreed audit purposes, in accordance with UK GDPR and applicable data protection requirements.

The Audit Team maintains contact information and milestone dates for each audit. Access to this information is strictly limited to staff within the NHSE audit function, and where applicable, authorised personnel from any commissioned external organisation.

All documentation supplied by, or on behalf of, a data recipient is stored securely in NHSE systems with access strictly limited to authorised members of the Audit Team and essential support staff.

Information provided by the data recipient will be retained only for as long as necessary, in line with NHSE's approved records management retention schedule, after which it will be securely disposed of.

For further details on how NHSE processes personal data, including individuals rights under the UK GDPR, please refer to the NHSE Privacy Notice.

NHSE may be required to consider requests for information under the Freedom of Information Act 2000. Each request is assessed on an individual basis by the NHSE Freedom of Information team, who will take into account confidentiality, data protection, and public interest considerations. Where appropriate, the data recipient will be consulted before any disclosure is made.

2.10 Audit Interviews

Audits interviews are spread across a number of days and will usually involve a minimum of 2 auditors from NHSE. 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.

Where interviews are conducted remotely, attendees are encouraged to use their cameras when speaking, to support effective communication and engagement. However, this may be adapted to individual needs or accessibility requirements, provided that identity and role can be confirmed in another appropriate way.

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. Screenshots will not be taken by the Audit Team without prior agreement.

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 any areas further.

The Audit Team will conduct an evidence-based assessment of the data recipient's controls and environment where data supplied by NHSE resides. The Audit Team will undertake interviews with 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 3.

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

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 Audit Team may conduct a further review of their 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(s) 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 three working days after the closing meeting, except where the Lead Auditor agrees a different timeframe during the closing meeting.

The Audit Team will not review new material created 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 2.20).

If an audit identifies any matters of serious concern, the Audit Team will escalate these to the data recipient, the NHSE SIRO representative and/or other relevant NHSE stakeholders at the earliest opportunity, to enable timely consideration and determination of the appropriate remedial action. Definition of findings and opportunities for improvement

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

- agreement nonconformity
- organisation nonconformity
- observation
- follow-up
- opportunities for improvement

2.10.5 Agreement nonconformity

An agreement nonconformity is a failure to implement a requirement contained in a DSFC, SDE contract or DSA, or in a documented communication between NHSE 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 NHSE in writing) as to why such guidance is not applicable.

2.10.6 Organisation nonconformity

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

2.10.7 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 NHSE 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.

2.10.8 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. These will be followed up by the IG Risk and Assurance Team.

2.10.9 Opportunity for improvement

The Audit Team may identify opportunities for improvement which could help an organisation improve its controls or processes based on the Audit Team's experience and knowledge from other data sharing audits. These are provided for reference only and are not followed up by the Audit Team.

2.11 Headline findings to NHSE

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

This will be followed by an internal meeting with senior management including the SIRO representative, DAS representative and subject matter experts, where the findings will be discussed in further detail.

Any headline findings of a serious concern may be followed up by any member of NHSE outside the audit process.

2.12 Risk Statement

The Audit Team will provide an overall risk statement which will be included in the audit report. This is based upon the evidence presented during the audit and the type of data made available at the time of the audit.

The risk statement will be based on:

- the nature of the data in terms of potential identification which could cause harm or distress
- the application 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 2.19). 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 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 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.

2.14 NHSE 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 reviewed by representatives from DAS, Communications and IG Risk and Assurance. This review is done either via email or a meeting.

This provides an opportunity for other specialist teams within NHSE to offer advice and commentary on the draft audit report prior to its publication.

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

2.15 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 review is expected to be performed, see section 2.20. The data recipient will also be requested to complete an action plan which address all the findings, see section 2.17.

2.16 NHSE action resulting from an audit

If an audit identifies any matters of serious concern, the Audit Team will escalate these to the data recipient, the NHSE SIRO representative and/or other relevant NHSE stakeholders at the earliest opportunity, to enable timely consideration and determination of the appropriate remedial action.

2.17 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. An action plan template will be provided by the Audit Team to complete.

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.

2.18 Publication on Internet

The data sharing audit report will be published by the Audit Team on the external NHSE 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 pre-election periods and public holidays.

2.19 Timescales

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

Action	Responsibility of NHSE	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
Provision of data recipient 's documentation		As defined in the notification letter
Audit interviews	Agreed dates	
Headline findings meeting with NHSE Senior Managers	Within 15 working days of the closing meeting	
Draft audit report issued to data recipient for comment	Within 20 working days following the closing meeting	
Any comments on the draft audit report returned to Lead Auditor		Within 5 working days of receipt of draft audit report
Internal publication meeting	The publication meeting is typically within 4 weeks	
Final audit report produced and sent to the data recipient	At least 3 working days prior to the report being published on the NHSE website	
Provide annotated action plan	Attached and sent when the final report is provided to the data recipient	
Final audit report published on NHSE website	Typically, will be published within the same month as the publication meeting	
Completed Action Plan returned.		Within 10 working days following receipt.

Table 2: Audit Timings

2.20 Post audit review

2.20.1 Audits with low-risk statement

All findings will be followed up by the Information Governance (IG) Risk and Assurance team at NHSE to confirm the findings have been satisfactorily addressed. Where audits follow this process, no follow up post audit review report will be created or published.

2.20.2 Audit with medium, high or critical risk statement

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 NHSE. 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 NHSE, see section 2.16. If a data recipient fails to engage with communication from the Audit Team on the action plan and supporting evidence, then the SIRO representative will be notified.

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 open findings after the review will be handed over to the IG Risk and Assurance team at NHSE to progress as appropriate with the data recipient. The Audit Team will update the status of the findings on the action plan to one of the following:

Open	The finding has not been resolved and has now been handed over to the IG Risk and Assurance team to progress as appropriate with the data recipient.
Closed	The data recipient has provided the evidence to the Auditor to demonstrate that the finding has been suitably resolved
No longer applicable	The action no longer applies or is required. This may be due to circumstances that have changed within the organisation audited, or the DSA is no longer active. However, if the organisation is audited in the future, this action may be reviewed to check its applicability to the new DSA. This status must be agreed between the Auditee and Auditor For example: It is part of a future action, i.e. acknowledgement of NHSE on reports using NHSE data or development of internal processes. Internal process(es) are developed that affect the requirement of NHSE DSA(s) and contracts.

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

2.21 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 NHSE complaints procedure can be found at:
NHS England » Complaining to NHS England

2.22 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 with the final report to complete a feedback questionnaire.

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

3. Appendix A - Examples of Question and 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. The type of questions will vary depending on the mechanism of data sharing (i.e. whether it is data dissemination or data access).

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**
• 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?	• 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 NHSE and the infrastructure being used to process and store such data, identifying all data touchpoints	
Typical opening questions/requests	**Examples of evidence**
• 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?	• 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 NHSE • Sub-licencing arrangements

Access control	
Aim: Establish the controls and security measures in place to control access to the data	
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 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?	• 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**
• 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 NHSE?	• 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 NHSE • 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**
• 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?	• 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**
• Does the data recipient have a formal risk and issue management process? • Have IT, IG and project risks associated with the NHSE 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?	• 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