Cyber Assessment Framework–aligned Data Security and Protection Toolkit

Strengthening Assurance – Independent Assessment and Audit Framework

Creating a culture
of Improvement

Information and Technology
for better health and care

Final

18/12/24

Objective E – Using and sharing information appropriately

Description

The organisation ensures that information is used and shared lawfully and appropriately.

Overview of the underlying Principles

Principle E1: Transparency

Principle E2: Upholding the rights of individuals

Principle E3: Using and sharing information

Principle E4: Records management

Principle E1: Transparency

Description

The organisation is transparent about how it collects, uses, shares and stores information. Privacy notices are clear and easy for members of the public to access.

Overview of the underlying Contributing outcomes

Contributing outcome E1.a – Privacy and transparency information

Contributing outcome E1.a – Privacy and transparency information

Description

You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.

The expectation for this contributing outcome is **Partially Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved All the following statements are true:	Achieved All the following statements are true:
NA#1. Privacy information is either not available, incomplete, or out of date. NA#2. Privacy information is provided in a format that not all patients and service users are able to access. NA#3. Privacy information is unclear, overly complex or does not use accessible language.	PA#1. Your privacy information is complete and up to date, covering how data is used, what individuals' rights are and how they can exercise them. PA#2. Privacy information is easily accessible and provided in a range of formats for different audiences. PA#3. Privacy information is concise, in plain language and communicated in an effective way.	A#1. Your privacy information is complete and up to date, covering how data is used, what individuals' rights are and how they can exercise them. A#2. Privacy information is easily accessible and provided in a range of formats for different audiences. A#3. Privacy information is concise, in clear and plain language, communicated in an effective way and uses a layered approach. A#4. Your organisation publishes relevant data protection impact assessments or summaries of these so that the public can better understand how their data is used and protected. A#5. Your organisation effectively uses its communications channels to be transparent about its data use.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing – Partially Achieved

1. **Privacy information structure** - obtain the organisation's privacy policy or privacy notice, documenting whether it is concise, and written in clear and plain language. This includes:
    a) avoiding the use of technical terms and acronyms (PA#3)
    b) Ensuring information is clearly structured and delineated through headings and subheadings that make it easy for the reader to identify key information (PA#3)
2. **Privacy information contents -** Verify that the policy or notice includes:
    a) How data is collected (PA#1)
    b) What types of data are collected (PA#1)
    c) Who information is shared with (PA#1)
    d) Whether information is transferred outside the UK (PA#1)
    e) What are the organisation's lawful bases for using information (PA#1)
    f) How data is stored (PA#1)
    g) The data rights which individuals hold in relation to their data and how to exercise these rights. These rights will include some combination of the following: right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object to processing. (PA#1)
    h) How to complain (PA#1)
3. **Privacy information process** - verify that the organisation has a process for reviewing and updating privacy information wherever there are changes to the organisation's processing of personal data, and how it ensures the process is followed. Privacy information reviews should include key personnel such as the Data Protection Officer (DPO). (PA#1)
4. **Accessibility of privacy information** - obtain evidence that the organisation has produced additional forms of privacy information which are effective for different audiences. This may include publication formats (such as web, print, audio), variations in length, and privacy information being given verbally through interaction with staff. (PA#2)

Additional approach to testing – Achieved

1. **Privacy information layering:** Obtain the organisation's privacy information and verify that key information is provided in a short notice and links to expand sections and access a second layer of more detailed information(A#3)
2. **Transparency in data protection impact assessments** (DPIA)–
    a. Verify that the organisation has a process for deciding whether a summary DPIA should be publicly published each time they complete a DPIA. (A#4)
    b. At least some proportion of the organisation's DPIAs should have met the threshold determined by the organisation for public availability. Verify that these DPIAs are publicly accessible in summary form. (A#4)

3. **Transparency through communication channels** - enquire with the organisation as to the various communication channels it uses to be transparent about its data use beyond its legally mandated privacy information. Inspect any documentation that details what each channel has been used for, and by whom. Inspect a sample of evidence to verify that each channel has achieved a discernible benefit in making the organisation's data processing more transparent. (A#5)

Suggested documentation list – Partially Achieved

- Privacy information (which may be titled “privacy policy”, “privacy notice” or another variation)
- Documents supporting scheduled reviews and updates to privacy information
- Evidence of different formats of privacy information being provided, for example website, printed, audio, documentation supporting verbal sharing

Additional documentation for Achieved level

- Documents supporting process for publishing DPIA summaries
- DPIA summaries which have been shared with the public
- Documents showing which different communications channels have been used effectively to be more transparent with the public about the organisation’s data processing

Principle E2: Upholding the rights of individuals

Description

The organisation respects and supports individuals in exercising their information rights.

Overview of the underlying Contributing outcomes

Outcome E2.a – Managing data subject rights under UK GDPR

Outcome E2.b – Consent

Outcome E2.c - National data opt-out policy

Outcome E2.a – Managing data subject rights under UK GDPR

Description

You appropriately assess and manage information rights requests such as subject access, rectification and objections.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Information rights requests under UK GDPR are frequently not recognised or appropriately responded to. NA#2. Responsibility for responding to information rights requests has not been assigned to an appropriately trained member, or members, of staff.	*Partial achievement is not possible for this contributing outcome*	A#1. Your organisation appropriately recognises and responds to information rights requests. A#2. Relevant staff members recognise that individuals can make information rights requests, the different categories of requests, and what action they should take when they receive one. A#3. Responsibilities for information rights requests have been delegated to appropriately trained and resourced staff members who can manage them in line with legal requirements.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Information rights request** - obtain and inspect the documented process for responding to information rights request. Verify that the process includes:
    a) Initial identification of an information rights requests, reflecting organisational awareness that this could include requests to access information, objections to processing information, requests to rectify inaccurate information, requests to erase information, requests to restrict processing of information, requests to transfer personal information to other organisations. (A#1)
    b) assessment and verification of the identity of the requester (A#1)
    c) information gathering (A#1)
    d) responding to the request and documentation of the request for record keeping (A#1)
    e) This should be completed within one month of receipt of the request, or within three months in the case of specific complex requests that are determined on a case-by-case basis (A#1)
    f) Test an example of a request for information rights, such as asking for access to patient records under the right of access or asking for information in a patient record to be amended under the right to rectification, and verify that the adequate process was followed. (A#1)
2. **Delegation of staff responsibilities** - assess whether staff responsibilities have been defined and documented for all steps of the information rights request process, from initial receipt (A#2) to fulfilment (A#3)
3. **Staff training** - obtain evidence of the training undertaken or qualifications held by staff to ensure they have the knowledge and skills, or experience, required to fulfil their responsibilities:
    a) For staff roles likely to be the organisation's port of entry for information rights requests, training undertaken or experience should ensure they are able to identify the different categories of information requests and know what to do when they receive one (A#2)
    b) For staff roles likely to process and fulfil information rights requests, training undertaken or qualifications held or experience should ensure they understand regulatory and legal requirements around information rights requests, including where requests might need to be refused (A#3)

Suggested documentation

- Process for responding to information rights requests
- Proof of training undertaken, qualifications held, or experience acquired by staff members for responding to information rights requests

Outcome E2.b – Consent

Description

You have a good understanding of requirements around consent and privacy, including the common law duty of confidentiality, and use these to manage consent.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Relevant staff members are not familiar with the common law duty of confidentiality or privacy rights or do not understand when they need to ask for consent. NA#2. You either do not have a policy or procedures in place, or are unsure whether your existing policy or procedures are adequate to ensure that consent is managed appropriately. NA#3. Information provided to patients and service users about their consent under the common law duty of confidentiality is either not given or unclear. NA#4. You do not have a process for refreshing consent when necessary.	*Partial achievement is not possible for this contributing outcome*	A#1. Relevant staff members understand consent under the common law duty of confidentiality, when they can rely on implied consent, and when they need to ask for or refresh existing explicit consent. A#2. Your organisation has a policy and procedures to ensure that consent is managed appropriately, including any decisions made by the Caldicott Guardian. A#3. Information provided to patients and service users about the use and sharing of information and consent is appropriate and clear.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Public information on consent** - Obtain the organisation's transparency materials and exemplar communications with the public relating to consent for information sharing. Assess whether:
   a) They cover common scenarios where consent will be asked before information sharing (A#3)
   b) Any written materials use clear and plain language, avoiding the use of technical terms and acronyms (A#3)
   c) The organisation has defined appropriate written and verbal methods for asking for consent for information sharing which staff members can refer to when needed (A#3) Clear headings and sub-headings (A#3)
2. **Consent policies and procedures** - inspect any documents provided by the organisation relating to their policies and procedures for managing consent and assess whether they cover:
   a) The different scenarios where consent may be used as the organisation's basis for using and sharing information under UK GDPR and the Common Law Duty of Confidentiality (A#2)
   b) The organisation's processes for obtaining, withdrawing and maintaining a record of consent (A#2)
   c) The responsibilities of staff members for making justifiable decisions when deciding whether to seek patient consent, including when to involve Caldicott Guardian or equivalent senior staff members (A#2)
3. **Staff training** - obtain documents provided by the organisation showing how it has assured that staff are aware of how to appropriately manage requirements relating to consent, and assess whether they cover:
   a) The common law duty of confidentiality, tailored to the level of understanding required for a person's job role:
      i) for non-IG staff roles, this could be scenario-based awareness of situations where they have the implied consent of a patient, for example for direct care, and other situations where explicit consent may be needed, for example where information is being used to reasons outside of direct care (A#1)
      ii) for IG staff roles, this could be documentation showing how the common law duty of confidentiality has been considered by IG teams in previous decisions relating to whether or not to seek a patient's consent (A#1)
   b) How to appropriately obtain and keep records of consent where consent is needed (A#2)

Suggested documentation

- Documents showing organisation’s policies and processes relating to consent
- Public materials about consent (for example, privacy information)
- Records of consent
- Training materials
- Documents from steering group meetings

Outcome E2.c – National data opt-out policy

Description

A robust policy and system is in place to ensure opt-outs are correctly applied to the information being used and shared by your organisation.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Relevant staff members are unsure where individuals can opt-out of their data being processed. NA#2. You are not sure whether opt-outs have been appropriately applied to relevant data sets. NA#3. Your procedure is not robust enough to ensure that all opt-outs are applied and routinely refreshed. NA#4. You are unsure whether your organisation is fully compliant with the national data opt-out policy.	*Partial achievement is not possible for this contributing outcome*	A#1. Your organisation understands the circumstances under which opt-outs must be applied and has recorded its applications in the information assets and data flows register. A#2. Your organisation clearly communicates to the public where they can opt-out of their data being shared. A#3. You have robust procedures and an adequate technical solution in place to ensure opt-outs are correctly applied.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Privacy information** - obtain the organisation's privacy information and assess whether:
   a) It explains the National Data Opt-Out and links the reader to a more detailed explanation of how it works. (A#2)
   b) It is explained in an accessible way, with clear and concise text (A#2)
2. **Information asset register** - obtain and inspect the information asset register and verify that data opt-out has been clearly documented against relevant information assets. Take a sample of the applications (up to 3) to test that the applications have the opt outs recorded (A#1)
3. **Data flow register** - obtain and inspect the record of processing activities (RoPA) / the data flow register, and verify that data opt-outs are clearly documented as part of each flow (A#1)
4. **Process controls for opt-outs** - evaluate the methodology for processing opt-outs, and the technical controls in place to ensure this methodology is applied correctly across all information systems (A#3)
5. **Training for key staff** – evaluate the training provided to relevant staff to check it includes details on the procedures for opt-outs (A#3)

Suggested documentation

- Privacy information
- Information asset register
- Data flow register
- Methodology for processing opt-outs
- Technical controls for ensuring opt-outs are consistently applied
- Staff training for opt-outs

Principle E3: Using and sharing information

Description

The organisation uses and shares information appropriately.

Overview of the underlying Contributing outcomes

Outcome E3.a – Using and sharing information for direct care

Outcome E3.b – Using and sharing Information for other purposes

Outcome E3.a – Using and sharing information for direct care

Description

You lawfully and appropriately use and share information for direct care.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Relevant staff members do not understand what direct care is, the activities it covers and when they should use and share information to facilitate it. NA#2. Information is not always used or shared when it is needed for direct care. NA#3. Information being used or shared for direct care is either inadequate or excessive. NA#4. You are unsure whether individuals would reasonably expect their information to be used or shared in all instances where your organisation does so. NA#5. There are no arrangements in place for routine information sharing for direct care. NA#6. There is no process to share data for non-routine ad hoc direct care purposes, or it is not always followed.	*Partial achievement is not possible for this contributing outcome*	A#1. Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it. A#2. Information is used or shared for direct care when it is needed. A#3. Information which is used or shared for direct care is relevant and proportionate. A#4. When information is used or shared for direct care, individuals' reasonable expectations and right to respect for a private life are considered. A#5. Your organisation has a process in place to enable appropriate non-routine ad hoc data sharing for direct care purposes. A#6. There are appropriate arrangements in place for information sharing for direct care.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Policies and procedures -** obtain and inspect documents provided by the organisation showing how they manage information sharing for direct care and assess whether they cover:
   a) Scenarios where direct care information sharing can be handled by non-IG staff roles (A#2)
   b) Scenarios where direct care information sharing requires escalation to IG team or equivalent (A#2, A#6)
   c) How they ensure information sharing is necessary and proportionate (A#3)
   d) How they ensure individuals' reasonable expectations and right to respect for a private life are considered in sharing decisions where relevant (A#4)
2. **Staff awareness** - Obtain evidence of how the organisation:
   a) Identifies relevant staff roles who need to have an understanding of processes for direct care information sharing (A#1)
   b) Makes relevant staff aware of scenarios where they should share information for direct care (A#1, A#2)
   c) Makes relevant staff aware of scenarios where they should escalate direct care information sharing decisions to IG team or equivalent (A#1, A#2)
   d) Makes relevant staff aware of their obligation to only share information which is proportionate and relevant (A#3)
3. **Data sharing arrangements** - verify that:
   a) The organisation has agreed internal thresholds for direct care information sharing, which, when met, trigger a review of whether an arrangement such as a data sharing agreement, a sharing framework, a Data Protection Impact Assessment (DPIA), etc. is needed or would be beneficial (A#6)
   b) The organisation has procedures for ensuring that sharing arrangements for direct care appropriately cover the nature of the information being shared, ensuring sharing is appropriate and proportionate, and clarifying roles and responsibilities in the sharing (A#3, A#6)

Suggested documentation

- Evidence of policies and procedures for direct care information sharing
- Training needs analysis and materials used for staff awareness
- Documents related to data sharing arrangements for direct care

Outcome E3.b – Using and sharing Information for other purposes

Description

You lawfully and appropriately use and share information for purposes outside of direct care.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Relevant staff members are not aware of the circumstances under which information might be used or shared outside of direct care. NA#2. Your organisation's practices for using and sharing information for purposes outside of direct care do not satisfy legal requirements including the common law duty of confidentiality UK GDPR or individuals' right to respect for a private life. NA#3. Individuals are not appropriately informed when their information is used or shared for purposes outside of direct care. NA#4. There are no arrangements in place for routine information sharing outside of direct care. NA#5. You don't maintain an up-to-date disclosure log detailing requests for individuals' information for purposes outside of direct care and sharing decisions your organisation has made. NA#6. There is no record of the lawful basis for disclosures that you have made.	*Partial achievement is not possible for this contributing outcome*	A#1. Relevant staff members understand which of your organisation's activities for using and sharing information fall outside of direct care. A#2. Your organisation's practices for using and sharing information for purposes outside of direct care satisfy legal requirements including the common law duty of confidentiality, UK GDPR and individuals' right to respect for a private life. A#3. Your organisation clearly communicates to individuals where their information may be used or shared for purposes outside of direct care. A#4. You maintain a disclosure log which details requests for individuals' information for purposes outside of direct care and sharing decisions your organisation has made, including the lawful basis for the sharing where appropriate. A#5. There are appropriate arrangements in place for information sharing outside of direct care.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Policies and procedures** - obtain and inspect documents provided by the organisation showing how they manage information sharing for purposes outside of direct care and assess whether they cover:
   a) Scenarios where information sharing for purposes outside of direct care can be handled by non-information governance (IG) staff roles (A#2)
   b) Scenarios where information sharing for purposes outside of direct care requires escalation to IG team or equivalent (A#2)
   c) How considerations around the common law duty of confidentiality, UK GDPR and individuals' right to respect for a private life are factored into decision-making before information is shared (A#2)
2. **Staff awareness** - obtain evidence of how the organisation:
   a) Identifies relevant staff roles who need to have an understanding of processes for non-direct care information sharing (A#1)
   b) Makes relevant staff aware of scenarios where they should share information for non-direct care purposes, ensuring information is relevant and proportionate (A#1)
   c) Makes relevant staff aware of scenarios where they should escalate non-direct care information sharing decisions to IG team or equivalent (A#1)
   d) Makes relevant staff aware of scenarios where they may need to communicate non-direct care information sharing decisions to patients and service users (A#3)
3. **Communicating to individuals** - obtain and inspect the organisation's privacy information or equivalent, assessing whether it appropriately covers situations where information may be used or shared for purposes outside of direct care (A#3)
4. **Disclosure log** - obtain and inspect the disclosure log if relevant and assess whether it lists the requests for individuals' information for purposes outside of direct care. This document should also include the result of the decision, the accountable owner for the decision, lawful basis for making this decision and the length of time for which the sharing agreement may last (A#4)

Suggested documentation

- Evidence of policies and procedures for non-direct care information sharing
- Training needs analysis and materials used for staff awareness
- Privacy information or equivalent
- Documents related to data sharing arrangements for other purposes outside of direct care
- Disclosure log

Principle E4: Records management

Description

The organisation manages records in accordance with its professional obligations and the law.

Overview of the underlying Contributing outcomes

Outcome E4.a – Managing records

Outcome E4.b – Clinical coding

Outcome E4.a – Managing records

Description

You manage records in accordance with your organisation's professional obligations and the law.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:	Partially Achieved	Achieved All the following statements are true:
NA#1. Some records are not in the locations indicated on the record keeping system. NA#2. You do not have an approved process for disposing of records or it is not routinely followed. NA#3. You are keeping data that identifies individuals for longer than it is needed. NA#4. Your standards for record keeping are not in alignment with the Records Management Code of Practice.	*Partial achievement is not possible for this contributing outcome*	A#1. Your organisation understands legal and professional obligations for records management. A#2. You have a record keeping system implemented at the organisational level which covers every stage of the information lifecycle and arranges records into an appropriate classification scheme. A#3. Records are appraised at the end of their retention period and disposed of when appropriate. A#4. Data destruction can be evidenced via destruction certificates or equivalent. A#5. Your organisation has a robust process to ensure that data that identifies individuals is not kept for longer than necessary.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Records management policy** - obtain and inspect the records management policy (or equivalent), and assess whether it contains:
   a) A list of professional and legal obligations for records management (A#1)
   b) The stages of the information management's lifecycle, including generation and collection, classification, processing, archiving and disposal. For each stage, the policy should clearly document the responsibilities of each stakeholder including patients (A#2)
   c) A defined classification scheme, which is based on the type of data (for example financial data, patient data, etc), the sensitivity of data and the volume of data (A#2)
   d) A clear retention period, with ownership for disposal being clearly assigned; (A#3)
   e) A disposal process, including ownership, and the information and evidence which should be retained by the organisation relating to records disposal (A#4)
2. **Record locations** – verify how the organisation reduces the probability of records being filed and held in incorrect places on its records keeping systems (A#2)
3. **Records at the end of retention period** – obtain and inspect an example of a record or records which were appraised at the end of their retention period and disposed of where appropriate. This could be in the form of meeting minutes or documented evidence of disposal or transfer (A#3)
4. **Data destruction via third parties -** if the organisation uses a third party for data destruction, select a sample from the disposal list and confirm there is valid destruction certificates or equivalent evidence for all included in the sample (A#4)
5. **Record keeping system** - obtain evidence of the record keeping system in place at the organisation, and evaluate its implementation against the policy using a sample (A#2)
6. **Retention and disposal process** - obtain and inspect the process in place to ensure that data that identifies individuals is not kept for longer than necessary. This process should define what data can be used to identify individuals, should refer to the classification scheme and the retention period, and include clear ownership for ensuring data is disposed of once its retention period is up (A#5)

Suggested documentation

- Records Management Policy or equivalent
- Record keeping system
- Retention and disposal process
- Documented evidence of records disposed of

Outcome E4.b – Clinical coding

Description

You are committed to regularly evaluating and improving your organisation's coded clinical data.

The expectation for this contributing outcome is **Achieved.**

Indicators of good practice (IGP) achievement levels

Not Achieved At least one of the following is true:		**Partially Achieved**	**Achieved** All the following statements are true:	
NA#1.	Your clinical coding practices are not compliant with current national clinical coding standards for the ICD-10 and OPCS-4 classifications.	*Partial achievement is not possible for this contributing outcome*	A#1.	Your clinical coding practices are compliant with current national clinical coding standards for the ICD-10 and OPCS-4 classifications.

As documented in the introduction to this framework, independent assessors are expected to use their professional judgement when assessing organisations against the Cyber Assessment Framework (CAF).

The approach and documentation list described below provides guidance on how to conduct testing and should be adapted as appropriate in order to assess whether the NHS providers outcomes are effectively achieved.

Suggested approach to testing

1. **Clinical coding policy** - obtain and inspect the clinical coding policy or equivalent, and assess whether its requirements align with current national clinical coding standards for the ICD-10 and OPCS-4 classifications (A#1)
2. **Clinical coding implementation** - obtain and inspect evidence that coding practices are aligned with the clinical coding policy (A#1)
3. **Clinical coding audit documentation** - obtain and inspect evidence of clinical coding audit documentation, to ascertain if these have been undertaken in line with guidance (A#1)
4. **Staff training** - obtain and inspect evidence that staff which require clinical coding training have completed training within expected timeframes (A#1)

Suggested documentation

- Clinical coding policy
- Clinical coding practices
- Clinical coding audit documentation