A Question of Balance

Independent Assurance of Information Governance Returns

Evidence Review Guides

Department of Health

audit commission

NHS Mersey Internal Audit Agency

NHS South Coast Audit

Contents

Reviewing evidence

What does good evidence look like?

1 Evidence tends to fall into one of several types. Table 1 gives examples

Table 1 Typical Evidence Types

Evidence review guides are available to support auditors in reviewing the following evidence types:

Evidence Types	
• Policies	• Awareness Material
• Strategies	• Web Based Content
• Procedures	• Minutes
• Public Information	• Plans
• Codes of Conduct	• Job Descriptions
• Training Material	• Project Initiation

2 Evidence review guides give good practice criteria for certain evidence types.

3 They are generic in that, for example, there is one guide for policies and not several covering all the relevant policies that might exist in an organisation.

4 The guides comprise three short sections:

- Characteristics
- Tasks
- Questions

5 These are described briefly in the following section.

Characteristics

6 These set out aspects of good practice - for example this will include references to:

- approvals and sponsorship;
- maintenance, update and review cycles; and
- communication, distribution and availability where appropriate.

Tasks

7 These are activities you can undertake in order to assess the evidence, examples may include:

- consistency with other guidance;
- any relevant survey responses; and
- availability on intranet or elsewhere.

Questions

8 These may be used in interviews with staff. In the example of a code of conduct, questions might include:

- how can staff access the code;
- who approves the code; and
- how is the code covered during the induction of new staff.

9 Questions are primarily of the open type to avoid leading respondents or limiting them to single yes/no answers.

Using evidence review guides

10 The following is designed as guidance for auditors. Note that these sources of evidence typically refer to a range of requirements and levels. The tasks and questions cover all the requirements affected and are indicative examples of questions that may be asked or tasks that could be carried out. It is not intended to be prescriptive or used as a checklist to be worked through in its entirety.

11 Auditors should develop the annual audit based on prescribed key requirements from the Department of Health Informatics Directorate and a risk based assessment of the remaining requirements. From this selection of requirements, auditors should be selective on the amount of work they do to satisfy themselves that the assurance objectives from the audit framework are met.

Evidence Review Guides

ERG001 - Policies

Good practice guide for policies

Evidence Type	IG Policies
Characteristics	Policies will normally be approved by senior management or delegated group.
	Policies will be subject to formal and regular review, usually at least annually.
	Policies will be universally available to staff across a range of media.
	Compliance with policies will normally be monitored and tested.
	Policies are the basis for an IG training programme that should reference them clearly.
	To be effective, policies should supported by guidelines and procedures and be written in clear, plain English.
	Policies may be multiple (system specific) but should not be 'cloned' and should reflect specific risks and controls in line with their applicability. They should also have a degree of consistency.
	Policies should be referenced as part of system and network login scripts and staff may formally sign (or click) to acknowledge receipt and understanding.
Tasks	Review relevant survey responses on compliance with the policy.
	Check the intranet content - can you find the policy, is it current and accessible?
	Check for explicit references to policies in sample job descriptions.
	Check for policy references and extracts in local training material.
	Check policy review processes and/or relevant minutes of meetings
	Check signed acknowledgements of policies in staff records.
	Conduct an internet search on some selected text from a policy - does it match exactly with policies from other organisations? If so, is it a cloned policy or does it draw effectively on good practice while reflecting organisational risks and controls.
	Check intranet traffic for relevant content, are policies regularly accessed?
	Assess the policy for 'readability'.
Questions	How can staff access the code?
	How are changes to policies controlled?
	Who approves the policy?
	How comprehensive is the policy - does it reference or incorporate a range of other relevant procedures and guidance?
	How are staff in need of reasonable adjustments catered for?
	How is the policy covered during the induction of new staff?
	How are temporary staff and contractors included in policy awareness?
	How often is the policy updated and reviewed?
	How is compliance monitored?

ERG002 - Strategies

Good practice guide for strategies

Evidence Type	IG Strategies
Characteristics	Strategies will normally be approved by senior management or delegated group.
	Strategies will be subject to formal and periodic review.
	Strategies will be universally available to staff across a range of media and in summary form.
	Strategies are usually subject to consultation as part of their development and adoption.
	Strategies will include a number of key or strategic objectives.
	To be effective, strategies should shape policy objectives and the overall compliance framework.
	Strategies should be achievable in terms of improvement and timescales and should reflect the current culture and level of achievement in the organisation.
	Staff awareness of strategies should include strategic objectives but is usually less than for policies and other tactical and operational documents.
Tasks	Check the intranet content - can you find the strategy, is it current and accessible?
	Check policies and procedures, do these support strategic governance objectives?
	Review the strategic objectives for reasonableness.
Questions	Who signs off the strategy?
	When was the strategy last reviewed?
	How are staff in need of reasonable adjustments catered for?

ERG003 - Procedures

Good practice guide for procedures

Evidence Type	IG procedures
Characteristics	Procedures will normally be approved by senior management or delegated person or group such as the Senior Information Risk Owner (SIRO).
	Procedures will be subject to formal and regular review, usually at least annually.
	Procedures will be universally available to staff across a range of media.
	Compliance with procedures will normally be monitored and tested.
	Procedures are covered in the detail of any IG training programme that should cover them fully.
	Procedures should supported by guidelines where necessary, Procedures should be brief, simple and easy to understand; and written in clear, plain English.
	Procedures should be clearly version and change controlled.
	Procedures should include a process where staff operating them can provide feedback on their effectiveness and suggest improvements.
Tasks	Review relevant survey responses on knowledge and awareness of relevant procedures and guidance.
	Check the intranet content - can you find a specific procedure, is it current and accessible?
	Check for explicit references to procedures in policies.
	Check for procedure references and extracts in local training material.
	Check procedure review processes and/or relevant minutes of meetings.
	Check versions of procedures in use - are these up to date?
	Check intranet traffic for relevant content, are procedures regularly accessed?
	Assess the procedures for 'readability'.
Questions	How can staff raise an issue with a procedure?
	How are changes to procedures controlled?
	Who approves the creation, amendment and deletion of procedures?
	How are staff notified about changes to procedures in their work area?
	How are staff in need of reasonable adjustments catered for?
	How are procedures covered during the induction of new staff?
	How are temporary staff and contractors included in procedure updates?
	How are IG procedures integrated and embedded with wider operating procedures?
	How is compliance monitored?

ERG004 - Public Information

Good practice guide for public information

Evidence Type	Public Information
Characteristics	Patient information will be concise, easy to read and written in plain language.
	Patients requiring reasonable adjustments will be catered for.
	The organisation will have considered and made arrangements for patients from BME communities, for example alternative language versions.
	Patient information will be available at a range of touch points - not necessarily those associated with the organisation.
	Patients should be able to provide feedback on patient information and make suggestions for improvement.
	Patient information should have clear contact details for patients requiring further information, this should include web or email and telephone details.
Tasks	Sample a range of patient information for reference to accuracy and use of information.
	Check style and presentation of information for consistency.
	Check admissions/ attendance points for the availability of patient information.
	Sample patient feedback processes.
	Check alternative formats are available (e.g. large print, Braille, audio, other languages) for patients requiring reasonable adjustments.
Questions	What has the organisation done to ensure patient material is easy to read and written in a simple plain English?
	How is patient information made routinely available to those places that require it?
	How are decisions made about the inclusion of relevant material with other patient communication?
	What has been done to improve awareness of staff about the importance of verifying information about patients?
	What has been done to improve awareness of patients and the public about the importance of providing accurate information?
	How are patients requiring reasonable adjustments catered for?
	How often is material revised and reviewed - is there a rolling planned refresh?

ERG005 - Code of Conduct

Good practice guide for code of conduct

Evidence Type	IG Code of Conduct
Characteristics	Code of conduct will normally be approved by senior management or delegated group.
	Code of conduct will be subject to formal and regular review, usually at least annually.
	Code of conduct will be universally available to staff across a range of media.
	Code of conduct will form the basis of an ongoing awareness training programme for staff.
	Check whether the code is consistent with the following: • Confidentiality NHS Code of Practice Staff Responsibilities • NHS Care Record Guarantee for England Commitments • Caldicott Principles
Tasks	Review relevant survey responses on compliance with the code.
	Check the intranet content - can you find the code, is it current and accessible?
	Check code for explicit references to obtaining and observing patient consent regarding secondary use.
	Check usage records of the NHS IG Training Tool software.
	Check review process and/or relevant minutes of meetings.
	Check signed acknowledgements against staff records.
	Check intranet traffic for relevant content, is it regularly accessed?
	Review instances of non-compliance or failure in process including lessons learned.
Questions	How can staff access the code?
	How are changes to the code of practice controlled?
	Who approves the code?
	How comprehensive is the code - does it reference or incorporate a range of other relevant procedures? E.g. DPA procedures
	Is there an annual training plan for staff?
	How is the code covered during the induction of new staff?
	How are temporary staff and contractors included in code of conduct awareness?
	How often is the code updated and reviewed?
	How is compliance monitored?
	How are staff in need of reasonable adjustments catered for?

ERG006 - Training Material

Good practice guide for training material

Evidence Type	IG Training Material
Characteristics	Basic IG training will primarily be provided through the NHS IG Training Tool.
	Local training material will normally be approved by senior management or delegated group.
	Training material will be subject to formal and regular review, usually at least annually.
	Training material will be universally available to staff to meet a range of preferred learning styles.
	Where appropriate, training material will be suitably tailored to the needs of staff.
	Training material will reflect appropriate national guidance.
	Organisations will base training delivery plans on a comprehensive needs analysis and risk assessment rather than taking a 'sheep dip' approach.
	Training material will cover: • regular staff; • new joiners; and • contractors and other temporary staff.
Tasks	Review relevant survey responses on training.
	Check the intranet content - can you find the training material, is it current and accessible?
	Review the training material for coverage of sampled key requirements.
	Check usage records of the NHS IG Training Tool software.
	Check review process and/or relevant minutes of meetings.
	Review induction material - is IG training included?
	Review the organisation's training plan including any training needs analysis.
	Check network traffic for training content, is it regularly accessed?
Questions	How can staff access training material?
	How are changes to training material controlled?
	Who approves local training material?
	How tailored is the training - how does it incorporate local policies and procedures?
	How is IG reflected in annual training plans for staff?
	How is the training covered during the induction of new staff?
	How are temporary staff and contractors included in training?
	How often is the training material updated and reviewed?
	How do you measure effectiveness of training?
	How are staff in need of reasonable adjustments catered for?
	How does security incident and event monitoring drive training needs?

ERG007 - Awareness Material

Good practice guide for awareness material

Evidence Type	IG Awareness Material
Characteristics	Local awareness material will normally be approved by senior management or delegated group.
	Awareness material will be subject to formal and regular review, changing regularly to maintain interest.
	Awareness material will be universally available to staff across a range of media.
	Where appropriate, awareness material will be suitably tailored to the needs of staff.
	Awareness material will reflect appropriate national guidance.
	Organisations will base awareness campaigns based on national and local risk assessments.
	Awareness material will cover: • regular staff; • new joiners; • contractors and other temporary staff.
Tasks	Review relevant survey responses on awareness.
	Check the intranet content and look around you - can you find awareness material, is it current and obvious?
	Review the awareness material - are messages simple and clear.
	Review awareness material for consistency with policies, procedures and training.
	Check the review process and/or relevant minutes of meetings.
	Review induction material - is IG awareness included?
	Review the organisation's IG communications plan including for IG awareness.
Questions	How can you be sure that awareness material reaches all staff?
	How often is awareness material changed or refreshed?
	Who approves local awareness material?
	How are awareness campaigns driven? - e.g. local risk assessments
	How is IG awareness reflected in communication plans?
	How is IG awareness covered during the induction of new staff?
	How is IG awareness covered for temporary staff and contractors?
	What input or feedback do staff have on awareness material?
	How do you measure effectiveness of awareness campaigns?
	How are staff in need of reasonable adjustments catered for?
	How does security incident and event monitoring drive awareness campaigns?

ERG008 - Web Based Content

Good practice guide for web based content

Evidence Type	**Web Based Content**
Characteristics	Availability of policies and procedures on line.
	Effectiveness of search results.
	Currency of information.
	Ability of users to challenge and comment.
	Ability to personalise content.
Tasks	Check to see if relevant policies and procedures are available.
	Check effectiveness of a search for “SIRO” - are the top five search results relevant?
	Test accessibility - can colours be changed and text scaled, is a text only version available?
	Check currency of information - when was the information last updated?
	Does the content have a named owner?
	Are comments allowed on intranet content?
	Can content be customised and alerts/ RSS feeds set up?
Questions	When was the relevant intranet information last updated or reviewed?
	How are staff in need of reasonable adjustments catered for (does the intranet meet minimum W3C accessibility standards)?
	Who approves local web content material?
	How often is the training material updated and reviewed?
	How do you measure effectiveness of web content?

ERG009 - Minutes

Good practice guide for minutes

Evidence Type	**Minutes**
Characteristics	There will usually be an agreed type of minutes for each meeting (e.g. action or full) and these will comply with an organisational template or standard.
	Minutes will be made available as soon as possible after the meeting.
	Confidential, personal or sensitive information is excluded from minutes unless these carry an appropriate security classification.
	Minutes may be made available on line as well as in hard copy.
	Formal minutes should be signed once these have been agreed.
	Minutes record key information about the meeting as well as the content (date, attendees, apologies etc).
	Attendees should be given the opportunity to comment on a draft before these are agreed.
	Previous minutes should be reviewed and agreed at the start of the following meeting.
	Minutes should take into account DPA and FoI requirements and form part of a publication scheme where appropriate.
	Action points should be clear with nominated persons and dates for completion.
Tasks	Review minutes for consistency of attendance.
	Check the intranet content - can you find a minutes from relevant IGT meetings or the Board, are these current and accessible?
	Check that minutes are signed off as agreed.
	Check minutes for house style and consistency.
	Check minutes for clearance of action points that are carried forward.
	Assess minutes for 'readability'.
Questions	How quickly are minutes produced?
	How are changes to minutes version controlled?
	How are minutes circulated, agreed and approved?
	How are staff notified about key messages from minutes?
	How are staff in need of reasonable adjustments catered for?

ERG010 - Plans

Good practice guide for plans

Evidence Type	IG Plans
Characteristics	Plans will normally be approved by senior management or delegated person or group such as the SIRO.
	Plans will be subject to continuous review, they are living documents.
	Plans will be available to key staff and stakeholders across a range of media.
	Plans will identify resources, key milestones and dependencies.
	Plans should be strictly version and change controlled.
	Plans are usually consistent in approach through the use of one or more templates or planning tools.
Tasks	Ask owners of plans to talk you through a sample of them.
	Ask for a critical path analysis to accompany project plans.
	Check plans against a baseline version to assess variance.
	Check versions of plans - are these up to date?
	Check a range of plans for consistency of approach?
	Assess the plans for credibility e.g. over-allocation of resources
Questions	How are stakeholders engaged in planning?
	How are changes to plans controlled?
	Who approves the creation and changes to plans?
	Are tolerance principles in use on plans to manage by exception?

ERG011 - Job Descriptions

Good practice guide for job descriptions

Evidence Type	Job Descriptions
Characteristics	For staff in general - compliance with relevant IG policies is explicitly referenced in job descriptions?
	Job descriptions for staff with specialist assurance roles also include the general statement on compliance with relevant IG policies?
	Job descriptions are subject to periodic review, at least annually as part of objective setting, appraisal and performance management.
	Objectives included in job descriptions are SMART.[i]
	Job descriptions are documented and accessible by staff.
	Job descriptions are agreed by job holders.
Tasks	Check that staff with specific information assurance assignments have an explicit reference to these assignments in their job description.
	Check a sample of job descriptions for key staff with specialist assurance roles to determine when these were last reviewed?
Questions	How does the organisation achieve consistency on including information governance responsibilities for non-specialist staff in job descriptions?
	How often are job descriptions subject to review, how is this linked to annual appraisal and performance management of staff?

[i] SMART - Simple, Measurable, Achievable, Realistic and Time bound

ERG012 - Project Initiation

Good practice guide for project initiation

Evidence Type	Project Initiation
Characteristics	Project initiation will include one or more aspects of information governance.
	All new system requirements will have a privacy impact assessment as part of project initiation.
	IG issues such as access controls, data classification, compliance and encryption are a mandatory element of project initiation documents for new and changed information systems.
Tasks	Review project initiation documents for evidence of IG issues.
	Review project management procedures for inclusion of review of IG issues mandated as a requirement for approval.
Questions	How are IG stakeholders incorporated in projects?
	How does the SIRO operate effectively across business change programmes and projects?