A Question of Balance

Independent Assurance of Information Governance Returns

Audit Requirement Sheets

DH Department of Health

audit commission

NHS Mersey Internal Audit Agency

NHS South Coast Audit

Contents

Scope

How to use the audit requirement sheets

1 These audit requirement sheets should be used in conjunction with the "Guidance for Internal Auditors", the “Evidence Review Guides”, the “Staff Survey” and the individual IG Requirements to assist you in scoping and reviewing evidence in support of your opinion with regard to the organisation's IG Toolkit return.

Which organisations are covered by this audit?

- Primary Care Trusts
- Acute Trusts
- Foundation Trusts
- Mental Health Trusts
- Ambulance Trusts
- Strategic Health Authorities

2 Note that GPs, Dental Practices and Social Care organisations are not included within the scope of this audit.

Which IG Requirements are covered?

3 There is a sheet for every requirement that applies to the in-scope organisations for the following series:

- **8100 Series** - Information Governance Management
- **8200 Series** - Confidentiality and Data Protection Assurance
- **8300 Series** - Information Security Assurance
- **8400 Series** - Clinical Information Assurance

4 Note that there are no audit worksheets for the 8500 (Secondary Use) and 8600 (Corporate Information) series. These requirements are out of scope for the audit for 2010-11.

5 Each worksheet provides you with the following information:

- a summary of each requirement;
- objective of the requirement; and
- a reference knowledge check.

6 Where appropriate, some of the above information is taken from the relevant IG Toolkit requirement and is repeated for ease of reference.

7 Worksheets also include a detailed section on assurance and evidence which is explained in the next section.

Evidence

Sources of assurance

8 Sources of assurance are set out for the three attainment levels, and where appropriate, expand on the information in the individual IG Requirements.

Criterion

9 This is the auditor summary for each attainment level and it may differ slightly in wording from the IG Requirement level summary.

Assurance required

10 This sets out the audit objective - these provide a range of detailed examples of the sorts of assurance that you should be seeking to evidence. This is not an exhaustive check list and as auditors, you must use your professional and local judgement to assess the controls in place, their operation and whether they achieve the objectives of the requirements and criteria.

Sources of assurance/ evidence

11 This sets out examples of evidence and will incorporate evidence referenced in the IG Requirement Checklist but, where appropriate, expands and extends this. As stated already, this is not a definitive check list to work through but it is indicative and represents the type of evidence that supports the assurance required. Note that there is no direct correlation between evidence and assurance required. A piece of evidence may directly support a single assurance requirement, it may support several requirements (directly or indirectly), or it may contribute to the overall criterion but not be specific to an assurance requirement.

What does good evidence look like?

12 Evidence tends to fall into one of several types. To support your work, there is a separate set of Evidence Review Guides (Table 1) which give good practice criteria for these evidence types. The guides 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.

Table 1 Typical Evidence Types

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

ERG Ref	Evidence Types	ERG Ref	Evidence Types
ERG001	Policies	ERG007	Awareness Material
ERG002	Strategies	ERG008	Web Based Content
ERG003	Procedures	ERG009	Minutes
ERG004	Public Information	ERG010	Plans
ERG005	Code of Conduct	ERG011	Job Descriptions
ERG006	Training Material	ERG012	Project Initiation

Evidence and attainment levels

13 Information governance scores are based upon the principle of a maturity model. In order to score at any given level the organisation must not only meet the criterion at that particular level but also of all levels below it.

- **Level one activities:** are assessed as the ‘planning stage’. These may include actual activity that contributes directly or indirectly towards the achievement of the requirement but it is still classed as planning - for example data collection or the establishment of appropriate arrangements. Initial stages of implementation may also be assessed as level 1.
- **Level two activities:** are assessed as the ‘doing stage’. Activities highlighted at this stage should directly contribute to the achievement of the requirement; for example, this is where policies are disseminated and implemented, training is delivered and staff briefings are held. It is expected that the requirement will have largely been met to achieve level 2 compliance.
- **Level three activities:** are assessed as the ‘check and act stage’. To be effective, activities against level three must provide demonstrable evidence of learning and improvement arising from review. Establishing a monitoring process or testing compliance is not sufficient to achieve a level three; identification of learning and implementing a planned improvement process is necessary in order to achieve the requirement.

14 The IG Toolkit attainment levels broadly follow this structure but there are a few exceptions to this, these are at the discretion of the Department of Health.

Judgement

Exercising professional judgement

15 It is important that organisations, and their auditors, look beyond the 'black and white' of the requirements and the criteria to ensure that they work within the spirit of them. Rather than being able to meet the specific documented criteria, they should be able to achieve the implicit objective.

16 Auditors will need to apply a degree of flexibility in their assessments to ensure that intended objectives are met, rather than checklist compliance being achieved. The guidance provided in the audit requirements Appendices 1 to 4) is intended to be indicative. It represents examples of the types of assurance or evidence and the ways in which they may be obtained. It is not intended that an organisation must be able to demonstrate evidence of each, nor is it intended that these should be the sole indicators. Auditors must be able to apply professional and local judgement to assess the controls in place, their operation and whether they achieve the objectives of the requirements and criteria.

17 Just because an organisation does not have or does not comply with one or more items of evidence on the audit requirement, this does not necessarily mean it cannot achieve the indicated attainment level. You must use professional judgement and review as much evidence as you deem necessary to satisfy yourself that the assurance required is sufficient to meet the criterion and the IG Requirement objective.

18 Equally, an item of evidence not listed in the audit requirement may have a bearing on your opinion for a particular IG Requirement. Just because it is not listed does not mean you cannot consider it; if it is of sufficient importance.

Documentation and records

19 Auditors should document their findings and maintain relevant working papers in line with local audit protocols and relevant local and professional standards.

More information

20 For more information on reporting the audit, assessing requirements and giving an overall opinion, please refer to the "Guidance for Internal Auditors".

Appendix 1 – 8100 Series

Information Governance Management - IG Framework (8101)

No.	IG Requirement
8101	There is an adequate information governance management framework to support the current and evolving information governance agenda.

Objective of the requirement

21 Formal accountability for information governance at senior and Board levels, supported by an effective organisation-wide framework of information governance that engages with staff at all levels.

Reference knowledge for auditors

22 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: What You Should Know About Information Governance Booklet 2010
- DH: NHS IG - Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents 2010
- DH: NHS Operating Framework for England for 2010/11

Table 2 Assurance required

Requirement 8101 - IG Framework

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Documented plans for the comprehensive review and documentation of information governance are in place, the work is led by a nominated senior manager as IG Lead.	Auditors require assurance that: • A suitably senior manager is formally responsible as IG Lead. • A documented information governance framework is in place or a documented plan exists to develop one. • The actual or planned framework is sufficiently comprehensive.	• Senior Manager job description with explicit objectives that reference the role of the IG Lead. • Board minutes or other papers setting out IG Lead responsibilities, assigned to a named individual. • A comprehensive documented IG framework, this may be in draft form or subject to formal approval. • The IG framework should include named resources.
2	The IG framework is approved at Board level (or suitably delegated senior manager); key governance structures and groups are established and operational.	Auditors require assurance that: • The Board (or formally delegated senior manager/ group) have formally approved the framework. • Accountability for sign-off is clearly documented to a named individual or authorised body. • Information governance bodies and groups have agreed and documented terms of reference. • Governance bodies are actively contributing to improvements in information governance.	As level 1 plus:[i] • Documented sign-off of the IG Framework that is clearly attributable to the Board or an authorised individual or group. • Current terms of reference for IG Bodies responsible for operating the IG Framework. • Minutes of meetings from IG Bodies responsible for operating the IG Framework. • Action plans or evidence of other process, policy or procedure change led by IG bodies.

[i] A plan to implement an IG Framework is not sufficient for attainment level 2; a documented IG Framework must be in place.

Appendix 1 – 8100 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Senior managers are briefed routinely on IG matters; briefings are documented and record action to secure learning and improvement. Effective review processes are established at least annually.	Auditors require assurance that: • Briefings and reports are prepared, submitted and discussed by the Board or delegated senior management. • The Board or suitable delegated senior management take and document decisive action on recommendations and improvements. • Learning is captured, documented and fed into improvement plans, training and awareness programmes. • Authorised IG Bodies are subject to appraisal and review of their terms of reference and effectiveness, either through self-assessment, peer review or other review process.	As level 2 plus: • Board minutes and associated relevant papers. • IG briefings and reports. • SIRO annual report for the SiC to the Accounting Officer.[i] • IG improvement plans. • Controlled changes to training and awareness programmes. • Documented reviews of terms of reference and effectiveness of IG Bodies, that result in action for improvement.

[i] Cabinet Office guidance states that the SIRO produces a report annually for the statement on internal control.

Information Governance Management - Policies, Strategies and Plans (8105)

No.	IG Requirement
8105	There are approved and comprehensive information governance policies with associated strategies and/ or improvement plans.

Objective of the requirement

23 Through the production, senior sponsorship and effective communication of information governance policies and strategies, staff understand both the cultural and practical aspects of compliance related to the job that they do.

Reference knowledge for auditors

24 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Confidentiality NHS Code of Practice 2003
- DH: Records Management NHS Code of Practice 2006
- DH: Records Management Roadmap
- DH: NHS Information Security Code of Practice 2007
- IC: Use and Disclosure of Health Data
- DH: NHS Operating Framework for England 2010/11

Table 3 Assurance required

Requirement 8105 - Policies, Strategies and Plans

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are comprehensive documented IG policies; these are approved by senior management or delegated group. Policy areas should include: • Information and Corporate Governance • Confidentiality, FOI and DP Acts • Records Management • Data Quality • Information Security	Auditors require assurance that: • A staff-oriented suite of IG policies exists. • Policies have been signed off by senior management or suitably delegated group. • Accountability for sign-off is included within policies and strategies.	• IG policy documents. • A documented record of the approval of this version of policies by the organisation's management board, or by a sub-group of the board. (If by a sub-group, evidence also of delegation of authority to this sub-group).
2	IG policies are available at appropriate points in the organisation and all staff members have been effectively informed about them and the need for compliance. Where appropriate, the guidance is tailored to particular staff groups or work areas. Policies are underpinned and supported by strategies and action plans which are signed off by senior management.	Auditors require assurance that: • Procedures exist to ensure that all existing and new staff have been made aware of the information governance policies and the need to comply. • IG policies are accessible across a range of media, including access for staff requiring reasonable adjustments[i]. • Staff know how to access the policies and the organisation can show that work has been done to disseminate them. • IG strategies and improvement plans link to policy review and organisational learning.	As level 1 plus: • Evidence that IG policies are available to staff at appropriate points in the organisation, such as an intranet or distribution to all appropriate departments. • Records of coverage of IG policy in awareness sessions, mandatory training, team discussions. • Record of the distribution of IG policies to staff with a signed acknowledgement. • Relevant web survey responses. • Improvement plans or evidence of other process, policy or procedure change sponsored by senior management.

[i] For example scalable fonts, large print, Braille or web content that can be used by a screen reader.

Appendix 1 – 8100 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Senior management annually review and approve IG policies, strategies and an integrated annual IG improvement plan. IG Policies are reviewed annually for alignment with latest guidance. Learning and action from review is identified and leads to controlled change to IG policies.	Auditors require assurance that: • IG policies are subject to on-going and regular review and maintenance. • Review is an active process that results in action such as controlled changes to policies, processes and procedures.	As level 2 plus: • Audit review of policies for content and alignment. • Meeting minutes or other papers from Management Board or delegated IG Groups. • Change logs or revised versions of IG policies and other key IG documents. • Organisational spot-checks on staff, to ensure that they understand IG policies and that they comply with them in their work. • Evidence of an integrated improvement plan to maintain compliance.

Information Governance Management - Third Party Contracts (8110)

No.	IG Requirement
8110	Formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.

Objective of the requirement

25 The organisation is assured that all contractors are made aware of the IG requirements incumbent upon them and that they are meeting these requirements.

26 Organisations are responsible for obtaining appropriate contractual assurance in respect of compliance with Information Governance (IG) requirements from all bodies that have access to the organisation's information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals.

Reference knowledge for auditors

27 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- ICO: Data Protection Audit Manual
- ICO: Outsourcing - A Guide for Small and Medium Sized Businesses
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- DH: Confidentiality NHS Code of Practice 2003
- DH: Records Management NHS Code of Practice 2006
- DH: Information Security NHS Code of Practice 2007
- BSI ISO/IEC 27000 Series of Information Security Standards

Table 4 Assurance required

Requirement 8110 - Third Party Contracts

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	All contractors or support organisations (including non-clinical staff) with access to the organisation's information assets have been identified and appropriate clauses for inclusion in contracts have been developed.	Auditors require assurance that: • The organisation has identified all contractors with access to information assets and that appropriate clauses have been included in all relevant contracts.[i]	• Evidence that the organisation has identified all third parties that may have access to information assets. • Evidence that the need for IG clauses on contracts has been assessed. • Where contracts need not include such clauses evidence that his has been risk assessed and accepted.
2	Appropriate clauses on compliance with IG have been put into all contracts and agreements.	Auditors require assurance that: • Appropriate descriptions of IG requirements are included in all relevant contracts with third parties. Note: The level of detail and content may vary from contractor to contractor dependent upon their level and nature of interaction with the organisation.	As Level 1 plus: • Evidence in relevant contracts of appropriate statement of IG requirements. • Evidence that there is a clear definition of how assurance will be received from the third party. • Where contracts do not include such clauses, evidence that his has been risk assessed and accepted.
3	Reviews and audits are conducted to obtain assurance that all third parties that have access to the organisation's information assets are complying with contractual IG requirements.	Auditors require assurance that: • The organisation has in place arrangements to test and assure that contractors are meeting their IG responsibilities as defined within the contracts.	As level 2 plus: • Key performance indicators have been established and are monitored e.g. incidents and breaches. • Any relevant certifications specified in the contracts (i.e. ISO27001) are maintained.

[i] Note: auditors need to ensure that the identification process identifies all those who could come into contact with information assets, not just as a direct part of their work but also through access to buildings and offices etc (Examples include: cleaners, security guards and couriers).

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			• Evidence that the organisation has received independent assurance reports, both in the form and from the source, stipulated in the contract. For example, internal audit reports or SAS70 reports and these indicate that standards are being met. • Evidence that any opportunities for improvement are included in action plans and the implementation of these plans is monitored to ensure effective implementation. • Evidence of feedback to relevant committees and groups through minutes and other meeting papers.

Information Governance Management - Employment Contracts (8111)

No.	IG Requirement
8111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation.

Objective of the requirement

28 The organisation is assured all the IG responsibilities of persons working on their behalf are clearly defined.

29 Organisations need to ensure that those undertaking work on behalf of the organisation do so in a lawful manner and meet all appropriate Information Governance (IG) requirements.

30 It is vital therefore that the contracts of permanent, temporary and locum staff contain clauses that clearly identify responsibilities for confidentiality, data protection and information security. Organisations must take reasonable steps to vet staff and provide IG training, or request appropriate training is undertaken, before permitting them to access systems and information assets.

Reference knowledge for auditors

31 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- BSI ISO/IEC 27000 Series of Information Security Standards
- NHS Employers: Recruitment and Retention - Employment Checks
- NHS Employers: Identity Check Standards
- DH: Confidentiality NHS Code of Practice 2003
- DH: Records Management NHS Code of Practice 2006
- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- Professional Codes of Confidentiality

Table 5 Assurance required

Requirement 8111 - Employment Contracts

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	All current and new employment contracts contain appropriate IG compliance requirements. An action plan has been documented to ensure that individuals working on behalf of the organisation understand their responsibilities.	Auditors require assurance that: • The organisation has clear IG related statements in contracts of employment with all staff whether permanent or temporary and that it has set out a route to ensure that these are understood by those concerned.	• Evidence that standard contract templates (both permanent and temporary) contain appropriate statements. • Evidence that the contracts of existing staff (both permanent and temporary) have appropriate clauses. • Assessment of the proportion and nature of current staff that haven't (or may not have) appropriate clauses in legacy contracts. • Evidence of planning for training of staff in the discharge of their requirements including plans for both standard and role-tailored training.
2	The action plan has been implemented and all existing staff are aware of their obligations for IG. All new staff are appropriately vetted, trained and provided with guidelines to ensure they are aware of their obligations for IG before they start handling person identifiable information.	Auditors require assurance that: • All staff have received appropriate training and are aware of their responsibilities.	As level 1 plus: • Reconciliation of training records to staff lists (including temporary staff). • Timing of the delivery of training to ensure that it is prior to the handling of information. • Relevant survey data - do staff understand their responsibilities? • Review of training materials for comprehensiveness and tailoring. • Evidence on HR records of appropriate vetting (for example CRB checks).

Appendix 1 – 8100 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Staff awareness of their responsibilities and their compliance with IG requirements is checked and monitored.	Auditors require assurance that: • The organisation has put in place arrangements to test whether staff have been trained and are aware or their responsibilities.[i]	As level 2 plus: • Key performance indicators have been established and are monitored at regular intervals (for example, attendance at training and test results). • Incident and event reports. • Evidence that the organisation, through internal or independent monitoring, has received assurances that procedures are being routinely applied and are achieving the desired outcomes. • Evidence that any opportunities for improvement are recorded in action plans and the implementation of these plans is monitored to ensure effective implementation. • Evidence of feedback to relevant committees and groups through minutes and other meeting papers.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Information Governance Management - Awareness and Training (8112)

No.	IG Requirement
8112	Information governance awareness and mandatory training procedures are in place and all staff are appropriately trained.

Objective of the requirement

32 All staff are appropriately trained on basic IG in line with the requirement to use the material contained in the national online NHS IG Training Tool supported by local material where necessary; basic IG training is integrated with induction training or new starters. Specialist and key staff needs are met through a needs-based approach.

Reference knowledge for auditors

33 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: NHS Operating Framework for England 2010/11
- DH: Informatics Planning 2010/11
- DH: What You Should Know About Information Governance Booklet 2010
- DH: Confidentiality NHS Code of Practice 2003
- DH: Records Management NHS Code of Practice 2006
- DH: NHS Information Security Code of Practice 2007
- DH: Information Governance Training 2010/11 briefing - July 2010

Table 6 Assurance required

Requirement 8112 - Awareness and Training

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A named individual, team or organisation leads on IG training for the organisation. A basic IG training programme is in place that is needs based and covers all permanent, temporary and contract staff (including new joiners). Staff in key or specialist roles are assessed for their specific additional training requirements. Training incorporates the NHS IG Training Tool and is supported by additional locally developed material.	Auditors require assurance that: • An effective IG training programme is in place that covers all staff, led by a suitable individual or team. • The IG training programme incorporates a basic package in line with national requirements that is suitable for all staff. • New starters are trained on IG as part of their induction. • Specialist and key staff training needs are assessed. • IG training programmes make best use of national material and organisations avoid unnecessary re-work or development.	• IG training plan. • Job description, team objective, SLA or other agreement to lead the delivery of IG training. • Induction training brief for new starters. • Sample needs assessments for specialist or key staff. • Training record of specialist or key staff. Additionally developed local material.[i] • Survey responses.
2	All staff complete basic IG Training in line with the agreed training programme. Key and specialist staff training needs are met. Training needs are regularly reviewed and re-evaluated.	Auditors require assurance that: • All staff have completed mandated basic IG training using the NHS IG Training Tool that complies with the training programme and staff are aware of their responsibilities. • Specialist and key staff training needs are met. • Specialist and key staff have been suitably trained.	As level 1 plus: • Survey responses. • Reports from the NHS IG Training Tool. • Training record of specialist or key staff. • Minutes from meetings and other papers.

[i] This should complement national material; it should not be excessive or duplicate existing material that is available nationally.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		• Training needs are regularly reviewed.	
3	Compliance checks and routine monitoring takes place. Learning outcomes from compliance checks are fed back into training needs assessments and the maintenance of the overall IGT training programme. The IG training programme remains fit for purpose in line with national policies and relevant legislation.	Auditors require assurance that: • Staff understand their responsibilities and act accordingly. • Learning from checks and reviews is captured. • Individual training needs arising from checks and reviews are identified and fulfilled. • Training programmes and needs assessments are adjusted to take account of learning from checks and reviews. • National changes to policy and law are incorporated into the training programme.	As level 2 plus: • Records of compliance checks and audits. • Action plan(s) to implement learning outcomes from compliance checks. • Records of attendance for additional or supplementary training. • Evidence of controlled change to the IG training programme and local training material.

Appendix 2 – 8200 Series

Confidentiality and Data Protection Assurance - Skills and Experience (8200)

No.	IG Requirement
8200	The information governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.

Objective of the requirement

34 To ensure that all relevant aspects of confidentiality and data protection are appropriately resourced through the appointment (or identification) and training of nominated individuals at appropriate levels of management; as part of wider information governance arrangements.

Reference knowledge for auditors

35 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Caldicott Guardian Manual 2010
- ICO: Data Protection Audit Manual
- DH: Confidentiality NHS Code of Practice 2003
- DH: What You Should Know About Information Governance Booklet 2010

Table 7 Assurance required

Requirement 8200 - Skills and Experience

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A nominated Caldicott Guardian is in post and with an approved plan and resources in place covering confidentiality and data protection work.	Auditors require assurance that: • A Caldicott Guardian has been appointed or nominated and assigned. • A plan to identify confidentiality and data protection work has been developed and endorsed by senior management. • Additional Caldicott resources have been identified or established.	• Named job description or formal assignment of responsibility. • Minutes or meeting papers documenting the assignment of responsibility. • A clear and detailed plan for the development of a confidentiality and data protection work programme, where none exists. This should include named resources, timescales, milestones and dependencies.
2	A confidentiality and data protection work programme is established together with the skills, knowledge, experience and resources to deliver it (including specialist external functions).	Auditors require assurance that: • An effective Caldicott function is established. • Staff with specialist confidentiality and data protection roles have been fully trained. • The confidentiality and data protection work programme is established and underway. • Outputs and formal reporting from the confidentiality and data protection work programme are produced and disseminated on a regular basis as a measure of accountability and effectiveness. • Specialist resources are available as required (e.g. legal services).	As level 1 plus • Training records for specialist and key staff. • Relevant survey responses on knowledge of DP legislation. • Formal terms of reference for a designated group to support or oversee the Caldicott function. • Contractual or other documented arrangements with external specialist suppliers. • Policies, strategies, improvement plans, logs and reports arising from the work of the Caldicott function.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	The work programme for the Caldicott function is integrated as part of overall IG, formally approved and regularly reviewed which drives improvement.	Auditors require assurance that: • The confidentiality and data protection work programme forms an integrated part of the wider information governance programme. • The senior nominated IG Forum or Board formally approve the work done which contributes to the annual IG improvement plan. • Confidentiality and data protection arrangements are reviewed annually for alignment with latest legislation and guidance. • Learning and action from review is identified and leads to controlled change to confidentiality and data protection arrangements.	As level 2 plus • Clear links between the plan for the confidentiality and data protection work programme and the corporate IG plan. The plan is monitored to ensure effective implementation. • Minutes of other meeting papers from the Board or delegated group reviewing and approving work done by the Caldicott function. • Application of learning outcomes from reviews of the confidentiality and data protection work programme. • Evidence of controlled change to the confidentiality and data protection work programme. • Evidence of planned review against changes to national guidance and relevant legislation.

Confidentiality and Data Protection Assurance - Staff Guidance (8201)

No.	IG Requirement
8201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users

Objective of the requirement

36 To maintain a confidentiality code of conduct.

37 Organisations have a legal duty to keep patient information confidential and secure. The provision of guidance to staff regarding individual responsibility for safeguarding and preserving confidentiality and information security will assist organisations to ensure their organisational duty is met.

Reference knowledge for auditors

38 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- CQC: Essential Standards of Quality and Safety
- GSCC: Code of Practice for Social Care Workers & Employers
- DH: Confidentiality NHS Code of Practice 2003
- The Caldicott Guardian Manual 2010
- Professional Codes of Confidentiality
- NIGB: The NHS Care Record Guarantee for England
- ICO: Guidance on the Issue of Monetary Penalties

Assurance required

Requirement 8201 - Staff Guidance

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is documented guidance for staff on keeping personal information secure and on respecting the confidentiality of service users that has been approved by senior management or committee.	Auditors require assurance that: • A staff-oriented confidentiality code of conduct exists. • The code of conduct has a legally recognised status within the organisation. • The code of conduct is legally binding on all staff. • The individual confidentiality responsibilities of each staff member are clearly and unambiguously defined. • Procedures are provided or referenced for the authorised disclosure of information. • The code of conduct complies with the requirements of the Data Protection Act, and NHS codes of practice; and • The code of conduct is available to all staff.	• Job description reflecting responsibility for confidentiality. • Agreed 'Terms of Reference' of a group assigned responsibility. • A staff confidentiality code of conduct exists as a controlled document. • A documented record of the approval of this version of the document by the organisation's management board, or by a sub-group of the board. (If by sub-group, evidence of delegation). • A code of conduct that complies with the staff responsibilities set out in the Confidentiality NHS Code of Practice, the commitments in the NHS Care Record Guarantee, and disclosure principles in the Caldicott Manual. • Evidence that the code of conduct is available to and accessible by staff at appropriate points in the organisation. E.g. via the intranet, or distribution to

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			appropriate departments.
2	The documented and approved staff guidance has been made available at appropriate points in the organisation and all staff members have been effectively informed about it and the need for compliance. Where appropriate the guidance is tailored to particular staff groups or work areas.	Auditors require assurance that: • The organisation has in place procedures to ensure that all existing and new staff have been made aware of the confidentiality code of conduct, and the need for their compliance with it. • Stronger assurance is required that all staff can easily view a copy of the code and that staff requiring reasonable adjustments[i] are catered for.	As level 1 plus: • Availability of the code of conduct on the intranet where there is one. • The code or references to it, in staff handbooks or documents distributed to all staff or departments. • Methods used to make all current staff aware of the need for confidentiality, and know how to access the code[ii]. • Documentary evidence that all staff have been reached, and so are aware of the need for confidentiality and of the code of conduct. • For all new joiners, evidence of induction training on confidentiality requirements, and code of conduct, or some other method of informing them.

[i] For example scalable fonts, large print, Braille or web content that can be used by a screen reader.

[ii] This might have many forms, such as awareness sessions, as part of mandatory training, team discussions, or distributions to all staff with signed acknowledgements.

Appendix 2 – 8200 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Staff compliance with the guidance on keeping personal information secure and on respecting the confidentiality of service users is monitored and assured. The staff guidance is reviewed regularly to ensure it remains aligned with policy and legislation.	Auditors require assurance that: • The organisation has in place robust processes to ensure that all staff understand the code of conduct and comply with it in all situations. This includes temporary staff and contract staff. • The code of conduct is subject to on-going and regular review and maintenance and that any specific needs of staff groups or work locations have been identified and appropriate guidance has been incorporated in the code.	As level 2 plus: • Organisational spot-checks on staff, to ensure they understand the code of conduct and comply with it.[i] • Organisational reviews of specific areas where patient information is requested or provided. • Results and materials used for patient satisfaction surveys and feedback. • Minutes of working groups or review meetings for the code of conduct. • Regular review of the code of conduct to confirm it aligns with central guidance and legal requirements. • Evidence of improvement actions to maintain compliance.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Confidentiality and Data Protection Assurance - Consent Prior To Use (8202)

No.	IG Requirement
8202	Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected.

Objective of the requirement

39 To control the use of personal information for purposes other than healthcare and respecting disclosure decisions.

40 There may be occasions when an organisation wishes to use patient information it has gathered for the purposes of providing treatment for another purpose, e.g. to a hospital Chaplain. To meet the legal requirements of the Data Protection Act 1998 and the common law, all organisations should ensure that they have procedures in place to gain specific informed consent to use that information for a secondary purpose. Organisations must also ensure that staff are aware of a patient's right to restrict disclosure of their personal information, and as far as possible ensure that this right is adhered to and respected, and that staff are aware of the possible disciplinary sanctions for a failure to respect patients' rights. Guidance for staff should be included within the confidentiality code of conduct necessary to achieve IG Requirement 8201.

Reference knowledge for auditors

41 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Confidentiality NHS Code of Practice 2003
- DH: Caldicott Guardian Manual 2010
- NIGB: NHS Care Record Guarantee for England
- ICO: Use and Disclosure of Health Data

Table 8 Assurance required

Requirement 8202 - Consent Prior to Use

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are guidelines for staff about appropriately seeking consent and respecting service user wishes and these have been approved by senior management or committee.	Auditors require assurance that: • The organisation has a confidentiality code of conduct that addresses the disclosure of patient information for secondary purposes (that is, not directly related to the health care of the patient). • The code gives guidelines on seeking and recording patient consent for such use. • The code requires the respecting of the patient's choice. • The code has a legally recognised status within the organisation. • The individual responsibilities of each staff member are clearly and unambiguously defined. • The code complies with the requirements of the Data Protection Act 1998, and relevant Codes of Practice. • The code includes guidelines for staff where an exemption to the requirement for consent may apply (for example raising the issue with the Caldicott Guardian or senior staff).	• Job description reflecting responsibility for confidentiality. • Agreed 'Terms of Reference' of a group assigned responsibility. • A version of the staff confidentiality code of conduct exists as a controlled document that addresses secondary uses of patient information. • A documented record of the approval of this version of the document by the organisation's management board, or by a sub-group of the board. (If by a sub-group, evidence also of delegation of authority to this sub-group). • Ensure that the code of conduct includes the obtaining and observing of patient consent or refusal of secondary use of patient information, compatible with the Confidentiality NHS Code of Practice, the commitments in the NHS Care Record Guarantee, and the disclosure principles in the Caldicott Guardian Manual.

Appendix 2 – 8200 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	The documented and approved guidelines have been made available at appropriate points in the organisation and all staff members have been effectively informed about the need to comply with them.	Auditors require assurance that: • The organisation has in place procedures to ensure all relevant staff are aware of the guidelines on seeking and observing patient consent on the secondary disclosure of patient information; and • All relevant staff can easily view a copy of the guidelines.	As level 1 plus: • Availability of the code of conduct/ practice (or guidelines) on the intranet, in staff handbooks, or in documents distributed to relevant staff. • Methods used to make all relevant staff aware of the code of practice, such as awareness sessions, as part of mandatory training, team discussions, or distributions to relevant staff with signed acknowledgements. • Documentary evidence that all relevant staff have been reached, and are aware and understand the consent guidelines. • For relevant new joiners, evidence of induction training on the consent guidelines, or some other method of informing them.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Staff compliance with the guidelines is monitored to ensure, unless there is a legal reason not to, they respect service user choices when consent to use or disclose personal information is required. The staff guidelines are reviewed regularly to ensure they remain aligned with policy and legislation.	Auditors require assurance that • The organisation has in place robust processes to ensure that all relevant staff understand the guidelines on patient consent for secondary disclosure of patient information. • The above process includes relevant temporary staff and contract staff; and • The organisation regularly undertakes sufficient sampling and/or monitoring to demonstrate that the observance of the guidelines is the normal situation.[I]	As level 2 plus: • Organisational spot-checks on relevant staff, to ensure that they understand the guidelines, and that they comply with it in their work.[II] • Organisational reviews of specific areas where secondary use of patient information is requested or provided. • Results and materials used for patient satisfaction surveys and feedback. • Incident logs of known failures to seek consent, or of disclosure without consent. • Minutes of task groups or risk committees reviewing exceptional cases. • Minutes of working groups or review meetings for the guidelines. • Evidence of regular review of the guidelines to confirm they are aligned to central guidance and legal requirements. • Evidence of improvement actions to maintain compliance.

[I] Auditors should examine any known cases of failure to observe the guidelines and the organisation's response to learn lessons and prevent recurrence.

[II] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Confidentiality and Data Protection Assurance - Proposed Use (8203)

No.	IG Requirement
8203	Individuals are informed about the proposed uses of their personal information.

Objective of the requirement

42 To effectively inform patients about confidentiality; the using of their information for a further purpose (see requirement 8202), and the importance of providing accurate information to NHS organisations (see also requirement 8402).

43 All organisations should have communication materials that clearly and concisely inform patients about confidentiality; the way that patient information is used and shared; and the importance of providing accurate information. This practice must be supported by active policy to ensure that patients are fully informed of the ways in general in which their personal information is used and in particular, when it is to be used for a purpose not originally envisaged when the information was first collected.

Reference knowledge for auditors

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Confidentiality NHS Code of Practice 2003
- Data Protection Act 1998
- NIGB: NHS Care Record Guarantee for England
- CQC: Essential Standards of Quality and Safety

Table 9 Assurance required

Requirement 8203 - Proposed Use

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	General communication materials are available to inform individuals accessing services about the use of their personal information.	Auditors require assurance that: • Patient communication materials are written in a simple style and layout suitable for most patients. • Patient communication materials describe the NHS understanding of confidentiality clearly and unambiguously and the need for patient information to be accurate (see also requirement 8402). • There are systems in place to ensure the production of materials, and the continuous availability at appropriate places; and • There are criteria for the distribution of materials with other patient communications.	• Information Governance policy and procedures describing communications with patients. • Example patient communications materials, for example leaflets and posters. • Equivalent material in the organisation’s public-facing web site. • Job descriptions covering the production and distribution of patient communication materials. • Standard procedure documents for the circulation and distribution of patient communication materials. • Policies and procedures on recording and checking patient information, available for example on the intranet, in staff handbooks, and/or standard procedure documents. • Training course descriptions and materials, from induction training, awareness sessions or training refresher courses.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	The general communication materials are supported by an active communications campaign to inform all individuals, including those with special/different needs, about how their personal information is used.	Auditors require assurance that: • There are systems in place to ensure the continuous availability of patient materials at all patient attendance points, such as reception desks at clinic, in-patient and out-patient wards, as appropriate. • There is more detailed information that can be made available to patients who request it. • The organisation has recently monitored patient understanding of patient information use and the need for information quality. • It is standard practice for front-line staff to verify information with patients and public on attendance/admission - see requirement 8402; and • The organisation seeks to ensure that all staff understand the need to maintain accurate patient information, and to respond appropriately to patients' enquiries.	As level 1 plus: • Examples of more detailed patient communications materials. • Patient awareness and satisfaction surveys on the management and quality of patient information. • Staff circulars and awareness surveys. • Minutes of working groups or committees reviewing the areas of patient information quality and communications to patients. • Job description(s) of individuals responsible for answering queries about the use of personal information. • Evidence of local assessment of types of materials required for service users. • Example patient communications materials in other formats (e.g. Braille, audio formats, large print), and in other languages. • Examples of recently revised and superseded communications materials. • Lists of available translators, readers and signers. • Guidance to staff on the availability of patient communications in other languages, other media and with human support.

Appendix 2 – 8200 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Staff compliance with their responsibilities to ensure individuals have access to the communications materials about the use of personal information is monitored and assured. The communications materials are reviewed regularly to ensure they remain aligned with policy and legislation.	Auditors require assurance that: • Patient communication materials clearly state the proposed uses of their personal information, and should include a fair processing notice to meet Data Protection requirements; • The organisation assesses the reasonable adjustments and different languages required by patients. The organisation provides and assesses suitable material and solutions to meet these needs. • The organisation regularly reviews its use of patient personal information, to identify any new uses of it, and to ensure that the organisation meets Data Protection requirements in respect of fair processing throughout the time that the information is held. • Affected patient groups are informed of new uses of their information, and where appropriate patient communications materials are updated to reflect the new usages. • There is periodic monitoring of whether staff observe the guidance on verifying patient/ public details.	As level 2 plus: • Job descriptions covering the updating and amending of patient communication materials. • Evidence of review of communications materials and improvement actions. • Results of recent or periodic needs assessments for communicating with patients, including patient awareness and satisfaction surveys for relevant groups.[i] • Results of random monitoring of staff information verification processes. • Terms of reference and reports from review processes, and working group or committee minutes showing decisions made.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Confidentiality and Data Protection Assurance - Access Request Procedures (8205)

No.	IG Requirement
8205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.

Objective of the requirement

44 To recognise and respond to a subject access request

45 Under section 7 of the Data Protection Act 1998, subject to certain conditions, an individual is entitled to be informed whether personal data about them is being processed by or on behalf of the data controller. If data is being processed, the individual has the right to be given a description of the data, the purposes of the processing and if the information is to be shared, who it will be shared with. The individual is also entitled to have access to the personal data held.

Reference knowledge for auditors

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- CQC: Essential Standards of Quality and Safety
- MoJ: Data Protection Pages
- Data Protection Act 1998
- Data Protection (Subject Access Modification) (Health) Order, 2000
- DH: Guidance for Access to Health Records Requests 2010
- NIGB: NHS Care Record Guarantee for England

Table 10 Assurance required

Requirement 8205 - Access Request Procedures

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a documented procedure for handling subject access requests that has been approved by senior management or committee. The procedure is designed to meet statutory deadlines.	Auditors require assurance that: • The documented procedures for handling subject access requests assign clear responsibility to a specified job role in the organisation. • The legal requirements and time limits for handling requests are clearly identified in the organisation's documentation. • Procedures are freely available throughout the organisation.	• Policy or standard procedure (named staff members) for handling subject access requests. • Availability of this, on the intranet, staff handbook, or other form of distribution to departments. • Job description for the job role which handles access requests. • Work plans allocating resources for dealing with subject access requests • Procedures have been approved by senior management (evidenced by minutes or other appropriate endorsement).
2	Subject access requests are actioned by fully trained and resourced staff. All staff members are aware of the need to support subject access requests, and where in the organisation such requests should be directed.	Auditors require assurance that: • The organisation has in place procedures to ensure that all existing and new staff have been made aware of the requirements, procedures and contacts for subject access requests. • The staff responsible for carrying out access requests are fully trained. • The time taken to carry out access requests is compatible with the total workload of the available staff. • Recent access requests have been carried out in conformance to statutory deadlines.	As level 1 plus: • Training records for staff carrying out subject access requests. • Records showing cases of subject access requests, and the time taken to complete them. • Methods used to make staff aware of how to direct subject access requests, and contacts. This might have many forms, such as awareness sessions, as part of mandatory training, team discussions, or distributions to staff. • Results of staff awareness testing for directing subject access requests.

Appendix 2 – 8200 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			• Offline evidence to demonstrate operation of procedures (e.g. log of subject access requests and their status).
3	The subject access procedure is regularly reviewed. Where necessary, additional measures have been implemented to assess and improve performance in meeting the statutory timeframes (or any more restricted timeframes required by the subject access request procedure.	Auditors require assurance that: • The organisation regularly undertakes sufficiently wide surveys, spot checks, and/or sampling to demonstrate that staff understand and comply with the procedures to handle or direct subject access requests. • The procedures to direct and to handle subject access requests are regularly reviewed. • There are procedures to measure and review the quality of the responses and time taken to carry out subject access requests.	As level 2 plus: • Results and materials used for surveys, random spot-checks or sampling of staff, on how to handle or direct subject access requests.[i] • Reports from monitoring the time taken to complete subject access requests. • Any responses or comments from requesters. • Minutes of working groups or committees that considered the working of the procedures. • Evidence of improvement actions arising from the review. (e.g. an improvement plan)

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Confidentiality and Data Protection Assurance - Confidentiality Audit Procedures (8206)

No.	IG Requirement
8206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information

Objective of the requirement

46 To monitor and audit access to confidential information.

47 The NHS Care Records Guarantee for England requires that all organisations that handle NHS information put in place mechanisms to ensure confidential information is protected. This requires access to confidential information to be monitored and audited locally and in particular requires that there are agreed procedures for investigating confidentiality events.

Reference knowledge for auditors

48 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- CQC: Essential Standards of Quality and Safety
- NIGB: NHS Care Record Guarantee for England

Table 11 Assurance required

Requirement 8206 - Confidentiality Audit Procedures

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been approved by senior management or committee and have been made available throughout the organisation.	Auditors require assurance that: • There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. • The procedures have been approved by senior management or committee and have been made available throughout the organisation.	• Policy on confidential patient information. • Standard procedures for monitoring and auditing access to patient information. • Management approval of procedures. (for example meeting minutes or other papers recording approval). • Documented assignment of responsibilities to job roles. • Corresponding job descriptions. • Publication of procedures throughout the organisation.
2	All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where confidentiality processes have been breached.	Auditors require assurance that: • The training provided for staff conducting audits and investigating alerts is comprehensive, clear and unambiguous on the action to be taken. • The written procedures for confidentiality audit and monitoring are implemented in the organisation. • Appropriate disciplinary and remedial actions are taken where confidentiality processes have been breached. • All staff members with the potential to access confidential patient information are	As level 1 plus: • Training records for staff carrying audits and investigations. • Descriptions of training provided. • Corporate security and human resources procedures. • Incident log of confidentiality alerts. • Reports of the subsequent disciplinary actions taken. • Minutes of committee reviewing confidentiality issues and performance.

[i] Note: Confidentiality events for audit include successful or failed attempts to access confidential information by unauthorised persons or for unauthorised purposes, security breaches such as shared passwords are an additional example.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		aware of the audit procedures; and • The audit procedures are widely accessible.[i]	• Availability of organisation's confidentiality, security and employment procedures to relevant staff. • Methods used to make relevant current staff aware of the confidentiality audit procedures and disciplinary sanctions. This might have many forms, such as awareness sessions, as part of mandatory training, team discussions, or distributions to staff. • For relevant new joiners, evidence of induction training on confidentiality requirements and audit.
3	Access to confidential personal information is regularly reviewed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality incidents or events.	Auditors require assurance that: • The procedures for confidentiality audits and monitoring are regularly reviewed for scope and depth. • Identified vulnerabilities are recorded, solutions are identified, and problems resolved; and • Staff effectiveness on confidentiality audits and monitoring is maintained, for example by appropriate on-going training.	As level 2 plus: • Reports from reviewing the audit and monitoring process.[i] • Security incidents and events related to confidentiality. • Risk register including identified confidentiality vulnerabilities. • Reports of procedural and/or security changes, resulting from alerts or identified risks. • Updated procedures and policy from lessons learned.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Confidentiality and Data Protection Assurance - Data Sharing Protocols (8207)

No.	IG Requirement
8207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations.

Objective of the requirement

49 To control the sharing of patient-identifiable information with other organisations.

50 The sharing of confidential patient-identifiable information should be governed by clear and transparent procedures that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations. In some circumstances these procedures and the underpinning standards should be set out within an agreed information sharing agreement or protocol.

Reference knowledge for auditors

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- CQC: Essential Standards of Quality and Safety
- Children's Act 2004
- DH: Confidentiality NHS Code of Practice 2003
- DH: Data Protection 1998 - Guidance to Social Services
- DH: Information Security NHS Code of Practice 2007
- DH: Records Management NHS Code of Practice 2006
- HM Government: Information Sharing Guidance
- Medical Research Council: Ethics and Research Guidance
- MoJ: Public Sector Data Sharing - Guidance on the Law
- NIGB: NHS Care Record Guarantee for England

Table 12 Assurance required

Requirement 8207 - Data Sharing Protocols

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A process has begun to identify and document the information requirements of each of the organisation's existing and new information sharing partners.	Auditors require assurance that: • There is a working list[I] of non-trusted recipients and/or suppliers of patient-identifiable data, for the organisation's activities. • For each case, the data required/provided and the justification for sharing the data are understood, and documented; and • There is a specific manager or group responsible for recording and maintaining this information.[II]	• Documented list of non-NHS information partners and the business needs served by exchanging information with them. • Job description of appointed manager. • Terms of reference of controlling committee or working group.
2	A high-level protocol approved by senior management or committee that sets out the basic information governance principles has been agreed with each of the organisations that are unable to demonstrate the required information governance performance and with those with whom personal information is routinely shared for non-care purposes.	Auditors require assurance that: • There is an extensive list of non-trusted recipients and/or suppliers of patient-identifiable data, for all of the organisation's activities (although sharing with trusted organisations for care purposes may be omitted). • For each case, the data required/provided and the justification for sharing the data are understood, and clearly and precisely documented. • The high-level protocol(s)[I] describe the principles and rules that will be followed,	As level 1 plus: • Copies of the agreed high level protocol(s). • Statements of compliance with the protocol(s).

[I] Organisations may choose to separately list cases of bulk data sharing (for example by controlled media exchange), and the sharing of information for specific patients (for example by letter or fax).

[II] For all bulk data sharing, and for individual exchanges to date, the actual partners should be identified, rather than generic titles such as "Social Services", "LEA", "care home" etc.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		consent procedures, legal compliance, security requirements etc. • There is a high level statement of compliance or similar, signed by both organisation’s Chief Executive and Caldicott Guardian (or equivalent), that binds the organisations into complying with the terms of the protocol.	
3	The high level protocol is augmented by specific sections which apply to each sharing partner so that there are appropriate protocols agreed with each of the organisations that are unable to demonstrate the required information governance performance and with those with whom personal information is routinely shared for non-care purposes. Additional protocols are agreed with all new information-sharing partners.	Auditors require assurance that: • There is detailed documentation associated with the information sharing protocol, for each partner with which there is bulk, periodic and/or frequent sharing of data. • These detailed protocols are formally agreed by both partner organisations. • There is a review process to ensure that new partner organisations are added when required, to regularly examine the working of the protocol, and update the protocols as required.	As level 2 plus: • Copies of the agreed information-sharing protocol(s). • Incident logs of any information governance issues relating to information sharing. • Reports and committee minutes identifying the addition of new organisations, and examining the working of the protocols and any information governance issues that ha

[i] Note: There may be a single umbrella high-level protocol, for all the data sharing organisations in the county or area. For each case of data sharing, there should be an indication of whether patient consent is required, or otherwise what legal requirement takes precedence.

Confidentiality and Data Protection Assurance - Processing Outside UK (8209)

No.	IG Requirement
8209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines.

Objective of the requirement

51 To protect the security of personal data transferred outside the United Kingdom.

52 The organisation is responsible for the security and confidentiality of personal information it processes. Processing may include the transfer of that information to countries outside of the UK, where this is the case organisations must comply with the Data Protection Act 1998 and Department of Health guidelines.

Reference knowledge for auditors

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- Data Protection Act 1998
- ICO: The Eighth Data Protection Principle and International Data Transfers
- ICO: International Transfers of Personal Information
- ICO: Data Protection Act 1998 - Legal Guidance

Table 13 Assurance required

Requirement 8209 - Processing Outside UK

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	All transfers of personal data to countries outside the UK have been documented, reviewed and tested to determine compliance with the Data Protection Act 1998 and Department of Health (DH) guidelines.	Auditors require assurance that: • For all the uses made of personal data by and for the organisation, and for transfers to other organisations for processing, the countries of data transit and of data processing have been determined and documented. • Where these countries are outside of the United Kingdom, compliance has been evaluated against the Data Protection Act 1998 (for example, the Eighth Data Protection Principle) and against current Department of Health (DH) guidelines. • Where these countries are outside of the United Kingdom, a documented report has been presented to senior managers, detailing the adequacy of data protection legislation in those countries.[i] • Where sufficient legal protection cannot be demonstrated, the organisation has approved actions to enable full compliance with the UK legal requirements and DH guidelines.	• Details of the personal data that is transferred to countries outside of the UK, and the countries of transfer. • Reports to senior management of the adequacy of legal protection for exported personal data. • Minutes of committee meetings authorising and delegating action to take measures to provide full protection, for example by contractual agreements. • Job description or other document assigning responsibility.

[i] Countries in the European Economic Area, and a few others, have been deemed by the European Union to have adequate levels of data protection.

Appendix 2 – 8200 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	All transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing transfers, the organisation ensures that new contractual arrangements are signed.	Auditors require assurance that: • Where necessary for transfers of personal data to countries outside of the United Kingdom, the organisation has obtained contractual protection for the confidentiality and security of the data. • For all transfers of personal data to countries outside of the United Kingdom, the current legal and contractual protection has been documented. • The organisation asserts that compliance has been achieved against the Data Protection Act 1998 and against current DH guidelines.	As level 1 plus: • Reports of the assessment of compliance with the Data Protection Act 1998 and DH guidelines.[i] • Documents covering contractual arrangements and amendments. • Meeting minutes covering decisions on contractual arrangements involving overseas transfer of data.
3	Transfers of personal data to non-UK countries are regularly reviewed to ensure they continue to fully comply with the Data Protection Act 1998 and DH guidelines.	Auditors require assurance that: • There are regular reviews of the transfers of personal data to non-UK countries, which evaluate continued compliance to the Data Protection Act 1998 and DH guidelines. • There is a procedure to ensure that new transfers of personal information are evaluated for country of processing, and compliance to the Data Protection Act 1998 and DH guidelines.	As level 2 plus: • Any action plan followed to secure compliance with the Data Protection Act 1998 and DH guidelines. • Reports from the review of current transfers of personal information.[ii] • The procedure to authorise new transfers of personal data. • Recent documented authorisation of any new transfers of personal data.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

[ii] As above

Confidentiality and Data Protection Assurance - Information Asset Security (8210)

No.	IG Requirement
8210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

Objective of the requirement

53 To ensure that new processes comply with Information Security, Information Quality and Confidentiality and Data Protection requirements.

54 The introduction of new processes could result in the organisation breaching information governance requirements. For best effect, requirements to ensure information security, confidentiality and data protection and information quality should be identified and agreed prior to the design, development and/or implementation of a new process or system.

Reference knowledge for auditors[i]

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Confidentiality NHS Code of Practice 2003
- NHS CFH: Good Practice Guidelines - Application Security *
- DH: Information Security NHS Code of Practice 2007
- DH: Records Management NHS Code of Practice 2006
- ICO: Privacy Impact Assessment Handbook
- BSI: ISO/IEC 27000 Series of Information Security Standards
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- BSI: ISO/IEC 20000-2:2005 Information Technology Service Management Code of Practice
- Data Protection Act 1998
- NHS CFH: Good Practice Guidelines - Information Security *

[i] Items marked (*) are available to NHS Network users only

Table 14 Assurance required

Requirement 8210 - Information Asset Security Compliance

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a documented procedure and structured approach for ensuring that new or proposed changes to organisational processes or information assets are identified and flagged with an appropriate information governance group or equivalent. Information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project cycle.	Regarding new processes,[I] or changes to existing processes, auditors require assurance that: • There are robust documented procedures to ensure that before any existing process is changed, in either clinical or non-clinical environments, the proposed changes are identified and reported to the appropriate information governance group for approval. • There is a process for the appropriate information governance group to be consulted before the introduction of new processes and information assets (preferably at the design stage).	• Procedures, guidance and forms for the introduction of new processes and information assets, in all business areas. • Terms of reference for each group in the organisation that considers information security, confidentiality and data protection, and information quality compliance issues.
2	All staff members who may be responsible for introducing changes to processes or information assets have been effectively informed about the requirement to seek approval from the appropriate group. All new implementations follow the documented project management process. Where the proposed new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate privacy impact assessment is always	Auditors require assurance that: • The information governance group considers new processes, and changes to existing ones, and asks for a formal impact assessment when it considers that there are new uses or significant changes to the handling of personal data. • Impact assessments consider the full range of information security, confidentiality and data protection, and information quality issues. • All staff responsible for introducing changes to processes have been informed of the	As level 1 plus: • Minutes of information governance groups considering new or changes to procedures. • Privacy impact assessments. • Methods used to make staff aware of the approval process. • Random checks of relevant staff to check their understanding of the guidance and their compliance to, the approval process. • Evidence of project management practice for implementing new

[I] This is for all processes, including the user functionality and visibility of data provided by automated processes such as computer programs and on-line services. It should not be at the discretion of staff whether to report any new or changed process to the information governance group.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
	carried out.	need to seek approval from the appropriate information governance group.	information assets.
3	Compliance with the guidance is monitored by reviewing any new processes or information assets that have been introduced. Project assurance processes are in place and the results are fed through project boards or similar groups. Remedial or improvement action is documented and taken where appropriate.	Auditors require assurance that: • For every new process and information asset, there is a thorough review to ensure that all NHS information security, confidentiality and data protection and information quality requirements and guidance are met. • There are checks to ensure that no processes or information assets have been introduced without review, and that the documented approval mechanisms have been followed. • The approval mechanism itself is reviewed, and staff guidance updated as necessary.	As level 2 plus: • Documented reviews of the operation of processes and information assets introduced over the past period that confirm compliance.

Appendix 3 – 8300 Series

Information Security Assurance - Skills and Experience (8300)

No.	IG Requirement
8300	The information governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.

Objective of the requirement

55 Skills knowledge and experience reflect the organisational needs and deliver adequate assurance.

Reference knowledge for auditors

56 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- BSI: ISO/IEC 27000 Series of Information Security Standards

Table 15 Assurance Required

Requirement 8300 - Skills and Experience

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	The role of Information Security Manager or Officer is assigned to a suitably qualified individual with an approved plan and resources in place covering information security assurance work.	Auditors require assurance that: • A suitably qualified information security manager or officer has been assigned. • A plan to identify information security assurance work has been developed and endorsed by senior management. • Additional information security assurance resources have been identified or established.	• Named job description or formal assignment of responsibility. • A clear and detailed plan for the development of an information security assurance work programme, where none exists. This should include named resources, timescales, milestones and dependencies. • Minutes or meeting papers documenting the assignment of responsibility and approval of the plan. • Evidence of professional qualifications and/ or membership of relevant professional bodies.[i]
2	An information security assurance work programme is established together with the skills, knowledge, experience and resources to deliver it (including specialist external functions). Responsibility is identified and documented across a range of staff roles.	Auditors require assurance that: • An effective information security assurance function is established. • Staff with specialist information security assurance roles have been fully trained. • The information security assurance work programme is established and underway. • Outputs and formal reporting from the information security assurance work programme are produced and disseminated on a regular basis as a measure of	As level 1 plus • Training records for specialist and key staff. • CPD log. • Relevant survey responses. • Service level or other documented agreements with providers of specialist resources. • Policies, strategies, improvement plans, logs and reports arising from the work of the information security

[i] For example CISM, CISA, CRISC or CISSP (or similar Information Security Professional accreditation) and ensure that, where appropriate, any continuous professional development requirements are maintained and up to date.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		accountability and effectiveness. • Specialist resources are available as required (these may be shared resources between organisations).	assurance function.
3	The work programme for the information security assurance function is integrated as part of overall IG work, formally approved and regularly reviewed which drives improvement.	Auditors require assurance that: • The information security assurance work programme is effectively incorporated within the broader IG work plan • Information risk forms an integrated part of the wider corporate risk arrangements. • The senior nominated IG Forum or Board formally approve the work done which contributes to the annual IG improvement plan. • information security assurance arrangements are reviewed annually for alignment with advances in technology as well as changes in legislation and guidance. • Learning and action from review is identified and leads to controlled change to confidentiality and data protection arrangements.	As level 2 plus • Clear links between the plan for the information security assurance work programme and the corporate IG plan. The plan is monitored to ensure effective implementation. • A clear and demonstrable link between IG and the wider organisational risk agenda (e.g. risk registers, assurance frameworks etc) • Minutes of other meeting papers from the Board or delegated group reviewing and approving work done by the information security assurance function. • Application of learning outcomes from reviews of the information security assurance programme. • Evidence of controlled change to information security assurance arrangements. • Evidence of planned review against technological developments, changes to national guidance and relevant legislation.

Information Security Assurance - Risk Management (8301)

No.	IG Requirement
8301	A formal information security risk assessment and management programme for key information assets has been documented, implemented and reviewed.

Objective of the requirement

57 To monitor and reduce risk to the organisation, person-identifiable information and critical information assets arising either from an absence, poor implementation or inadequate management of relevant controls over key information assets.

Reference knowledge for auditors

58 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- The NHS Information Governance Toolkit
- The NHS Information Security Code of Practice
- ISO27001:2005 & ISO27002: 2005 – The International Standards for Information Security Management Parts 1 and 2
- ISO27005: 2008 - Information Technology, Security Techniques, Information Security Risk Management
- The Confidentiality NHS Code of Practice
- DH Records Management NHS Code of Practice
- The NHS Information Risk Management: Good Practice Guide

Table 16 Assurance required

Requirement 8301 - Risk Management

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a documented plan and programme covering security risks to key information assets that has been approved by senior management or committee.	Auditors require assurance that: • Key information assets are defined. • a risk management programme and plan exists with a clearly defined scope. • All key information assets are within scope; • Senior management or suitably delegated approval is in place. • Arrangements are based on a formal risk assessment method. • The method is systematic to ensure inclusion of all in-scope assets. • The programme prioritises risks in line with business functions. • The programme considers information risks of business partners. • The programme and plan incorporates a review process. • The programme is accountable to the Senior Information Risk Owner (SIRO) and associated governance structures; and • The programme is formally linked to the corporate risk management arrangements.	• A risk management programme and plan as controlled documents. • Associated up to date and controlled strategies, policies and procedures. • An up to date register of key information assets. • Relevant information risk policies and procedures in line with other relevant IG Toolkit requirements • Documented approval of the plan and programme by the organisation’s management board, or by a sub-group of the Board. If by a sub-group, evidence also exists of delegation of authority. • Minutes from meetings or discussions with key staff as evidence that the programme and plan contribute to and are discussed regularly within governance structures. • Relevant web survey data.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	The information risk assessment and management programme is a core activity for the organisation.	Auditors require assurance that: • Key information assets have been risk assessed in line with business priorities. • Relevant strategies, policies and procedures have been disseminated to staff and staff understand how to follow them. • Awareness of and compliance with relevant strategies, policies and procedures is monitored. • Corporate risk arrangements reflect appropriate information risks. • Review processes are established to ensure that risk management is effective, current and embedded. • Risk management activity is reflected in ad-hoc reports and the annual assessment of information risk performance by the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO); and • The Accounting Officer has presented the annual assessment of information risk performance to the Board who have endorsed any recommendations for inclusion in the information risk management programme and plan.	As level 1 plus: • Sampled key information asset risk assessments. • Evidence of staff awareness and compliance training on relevant strategies, policies and procedures. • Corporate risk register. • Published risk management and compliance reviews. • IAO reports and SIRO annual assessment of information risk.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	The information risk management programme is reviewed regularly and the findings appropriately reported. Maintenance and documentation structures need to be reviewed regularly to ensure they remain current and aligned with policy and legislation	Auditors require assurance[i] that: • Compliance reviews and monitoring (e.g. spot checks) are carried out and learning is captured. • Results from reviews and monitoring are fed into the information risk programme and plan. • Arrangements and governance structures are reviewed at least annually to take account of changes to national policies, guidance and relevant legislation; and • Relevant strategies, policies; and procedures are regularly reviewed to take account of learning from compliance reviews and monitoring.	As level 2 plus: • Documented learning from organisational spot-checks on staff, to ensure information risks policies and procedures are complied with. • Changes to risk programme and plan (with derivation). • Changes to arrangements and governance structures (with derivation). • Minutes of relevant working groups or review meetings. • Documented improvement plans.

[i] In arriving at their opinion auditors need to ensure that information risk management isn't focused upon risk identification, assessment and logging; there needs to be a clear link to risk mitigation, control, monitoring and improvement.

Information Security Assurance - Incident Management (8302)

No.	IG Requirement
8302	There are documented information security incident/ event reporting and management procedures that are accessible to all staff.

Objective of the requirement

59 To minimise the impact and learn lessons from potential and actual security incidents and events through effective identification, reporting, documentation and investigation of such incidents. Remedial action should include action to ensure the prevention of any recurrence including corrections to the design of systems and the procedures that support their operation.

Reference knowledge for auditors

60 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- Matthew Swindells letter: Guidance on Defining and Reporting Serious Untoward Incidents (SUIs) dated 28th February 2008
- DH NHS IG: Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (Gateway Ref 13177)
- DH: NHS IG - Information Risk Management Good Practice Guide 2009
- DH: Information Security NHS Code of Practice 2007
- National Patient Safety Agency (NPSA) Tools
- BSI ISO/IEC 27000 Series of Information Security Standards

Table 17 Assurance required

Requirement 8302 - Incident Management

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are documented and approved processes for reporting, investigating and managing information security incidents and events.	Auditors require assurance that: • Documented policies and procedures for security event management are in place. • Policies and procedures have been reviewed and approved. • Approval and review is by senior management or suitably delegated group and includes the Senior Information Risk Owner, the Board (or formally delegated sub-group) and Information Asset Owners or equivalents). • Date of review and approval is recorded. • Approval is by a nominated signatory. • Period since last review does not exceed 12 months. • A communication plan is in place covering all relevant staff, external organisations and third party contracts. • Incident and event recording and logging systems are established, either in their own right or as part of other data capture systems. • Reporting and analysis requirements and relevant key performance indicators (KPIs) have been considered as part of system design; and, • There are links between incident and problem management processes in order that root causes may be identified and	• Relevant, up to date and controlled, policies and procedures. • An up to date register or record of third party contracts. • Up to date staff data as the basis for disseminating procedures and delivering training. • Documented review and approvals process by senior management or suitably delegated group and includes the Senior Information Risk Owner, the Board (or formally delegated sub-group) and Information Asset Owners or equivalents. • Minutes from meetings or discussions with key staff as evidence that the policies and procedures contribute to and are incorporated within governance structures.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		addressed where appropriate.	
2	The information security/ event reporting and management procedures have been communicated to staff and relevant third parties.	Auditors require assurance that: • Relevant policies and procedures have been disseminated to all staff and staff understand how to follow them. • Relevant policies and procedures have been disseminated to all third party contractors. • Relevant training has been provided to all staff to explain how policies and procedures should be followed. • Relevant training has been provided to all third party contractors to explain how policies and procedures should be followed; and • An on-going programme of security/event reporting awareness is in place for all employees of the organisation, both permanent and contract.	As level 1 plus: • Sampled incident and event reports. • Corporate training plans. • Examples of awareness material (i.e. posters, e-mail campaigns, network log-in script messages, intranet articles). • Inclusion of requirement to comply with relevant policies and procedures in third party contracts. • Relevant web survey data.
3	The SIRO and IAOs (or equivalent), monitor compliance with procedures, taking corrective action if evidence of non-compliance is discovered. Incident and event reports are analysed and where necessary, policies and procedures are reviewed to minimise recurrence. The procedures need to be reviewed	Auditors require assurance that: • Compliance reviews and monitoring (e.g. spot checks) are carried out and learning is captured. • Event and incident reports are analysed for trends as well as evidence of compliance and non-compliance. • Relevant policies; and procedures are regularly reviewed to take account of	As level 2 plus: • Documented learning from spot checks on staff, to ensure compliance with incident reporting policies. • Results of internal or self-audits[I]. • KPI's and trend analysis and other management reports from incident reporting. • Changes to relevant policies; and

[I] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
	regularly to ensure it remains aligned with policy and legislation.	learning from compliance reviews and monitoring.	procedures (with derivation). • Changes to arrangements and governance structures (with derivation). • Minutes of relevant working groups or review meetings.

Information Security Assurance - Registration Authority (8303)

No.	IG Requirement
8303	There are established business processes and procedures that satisfy the organisation’s obligations as a Registration Authority.

Objective of the requirement

61 To ensure that business process and supporting procedures meet the obligations placed upon the organisation as part of its registration responsibilities which are managed as a key information asset.

Reference knowledge for auditors[l]

- DH: Information Security NHS Code of Practice 2007
- NHS Employers: Recruitment and Retention - Employment Checks
- NHS Employers: Identity Check Standards
- NIGB: The NHS Care Record Guarantee for England
- DH: Records Management NHS Code of Practice 2006
- DH: Confidentiality NHS Code of Practice 2003
- NHS CFH: Registration Authorities - Operational Process Guidance *
- NHS CFH: Registration Authorities - Software Downloads *
- NHS CFH: Registration Authorities - User Leaflets *
- NHS CFH: Registration Authorities - Equipment & Specifications *
- NHS CFH: Registration Authorities - Building Workstations *

[l] Items marked (*) are accessible by NHS Network users only

Table 18 Assurance required

Requirement 8303 - Registration Authority (RA)

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Responsibility for RA is assigned at Board level or equivalent with an approved plan and resources in place covering the RA function.	Auditors require assurance that: • A suitably senior RA manager has been assigned. • Additional RA resources have been identified or established. • Responsibilities across the RA function are documented and approved at Board level. • A plan to assess organisational needs has been developed and endorsed by senior management. • Training needs have been assessed • Third part staff have been considered and included as part of any RA arrangements.	• Named job description or formal assignment of responsibility. • A clear and detailed plan across the RA function. This should include named resources, timescales, milestones and dependencies. • Board minutes or meeting papers documenting the assignment of responsibility and approval of the plan.
2	The RA plan and its associated operational aspects have been implemented and function effectively across the organisation.	Auditors require assurance that: • Training needs of staff have been analysed and a training programme is well underway. • RA equipment and consumables are adequately controlled with procedures in place for use and maintenance. • The RA process is effectively embedded as part of business as usual.	As level 1 plus • Evidence of attendance on a training programme designed to meet the needs of RA staff. • Review of training materials for comprehensiveness and tailoring. • Asset or configuration management records for smartcards (both hardware, software. • Review of documented authorisation process for new registrations, changes and revocations. • Separate or annexed security policy and supporting procedures applicable to RA assets.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Reliability and robustness of RA arrangements are subject regular audit and monitoring; learning is identified and applied to deliver improvements where necessary.	Auditors require assurance that: • Compliance audits and monitoring are carried out and learning is captured. • Security event and incident reports relating to RA arrangements are analysed for trends and non-compliance. • RA arrangements are regularly reviewed to take account of learning from compliance reviews and monitoring; and • Learning from review, audit and analysis delivers improvement.	As level 2 plus • Review of training to reflect changes in national policy and local learning from analysis of security incidents and events. • Training evaluation questionnaires and changes to training based on delegate feedback. • Outcomes from periodic audits that check controls over RA assets (includes controls over authorisation forms).[i] • Implementation of learning from maintenance and review processes - action plans or other evidence of changes made.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Information Security Assurance - Smartcards (8304)

No.	IG Requirement
8304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.

Objective of the requirement

62 To ensure that staff members and those working on behalf of the organisation, issued with an NHS smartcard, comply with the terms and conditions of issue.

63 Disciplinary procedures reflect how breaches of the conditions of issue will be dealt with.

Reference knowledge for auditors[l]

Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- NHS CFH: Registration Authorities - Governance Arrangements for NHS Organisations *
- NHS CFH: Registration Authorities and Smartcard Guidance
- NHS CFH: How to Register for a Care Record Service Smartcard Leaflet *
- NHS CFH: RA01 Short Form Conditions *

[l] Items marked (*) are accessible by NHS Network users only

Table 19 Assurance required

Requirement 8304 - Smartcards

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A plan has been developed and approved by senior management or committee for ensuring compliance with the terms and conditions of smartcard usage. The plan covers: • monitoring; • compliance; and • enforcement.	Auditors require assurance that: • A plan is in place to monitor and enforce user compliance in respect of smartcard usage. • The plan is documented. • The plan is linked to disciplinary processes. • The plan forms part of the overall RA implementation plan (see req. 8303) • The monitoring and enforcement plan has been approved by senior management.	• Job description, a note or email message assigning responsibility, or terms of reference of a group. • A clear and detailed compliance and monitoring plan for Smartcard use that links to the overall RA plan (see req. 8303). • Approval of the plan in meeting minutes, email or other written approval from a senior manager.
2	The plan and any associated procedures have been implemented. Smartcard users have been effectively informed and understand: • smartcard use will be monitored; • the need for compliance; and • sanctions for non-compliance.	Auditors require assurance that: • The procedures for dealing with breaches are accessible to users. • Staff members are aware that monitoring of their smartcard usage will take place. • Staff members are aware of the disciplinary measures that may be taken in the event of a breach.	As level 1 plus: • Procedures available to staff by electronic or printed means. (Intranet, Staff Handbook, etc). • Staff briefing materials. • Induction and training materials. • Induction and training records.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			• Relevant staff survey responses.
3	Monitoring of smartcard usage and staff compliance with the terms and conditions is carried out. Non-compliance results in remedial action. The monitoring and enforcement arrangements are reviewed annually and monitored in year.	Auditors require assurance that: • Monitoring of compliance takes place. • Actions are taken in the event of non-compliance. • Awareness of 'terms and conditions' is maintained. • Enforcement and compliance arrangements are regularly reviewed to ensure that they meet legislative and national requirements.	As level 2 plus: • Completed monitoring forms. • Monitoring or compliance reports.[i] • Evidence of improvement action taken arising from compliance checks. • Meeting notes that show discussion/ review of awareness material. • Documented formal review processes for relevant procedures.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Information Security Assurance - Access Controls (8305)

No.	IG Requirement
8305	Operating and application information systems (under the organisation's control) support appropriate access control functionality. Documented and managed access rights are in place for all users of these systems.

Objective of the requirement

64 Access to information systems and assets is controlled, staff are given access to the information and systems they need to do their job and no more. Registration, change and revocation of access is dealt with under formal procedures with strict control on administrator, supervisor and equivalent privileged user accounts.

Reference knowledge for auditors[l]

65 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management: Good Practice Guide 2009
- DH: NHS IG - Blogging and Social Networking 2009
- NHS CFH: Good Practice Guidelines - Application Security *
- NHS CFH: Good Practice Guidelines in Information Governance - Information Security *
- ISO/IEC 27000 Series of Information Security Standards

[l] Items marked (*) are accessible by NHS Network users only

Table 20 Assurance required

Requirement 8305 - Access Controls

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Requirements are in place for controlled access to key information systems and assets. Access rights have been agreed and documented for key information assets; these cover individual and group level access.	Auditors require assurance that: • Controls for key information systems and assets have been defined and responsibility has been assigned for managing access. • Security policies exist at the system level and are consistent with overall policies. • New build or major upgrade IT system projects routinely incorporate appropriate IG requirements as part of project initiation and system design.	• Job description, a note or email message assigning responsibility, or terms of reference of a group. • System security policies - check for consistency[I]. • Project initiation documentation. • Specifications for access controls and system designs.
2	Access to key information systems and assets is controlled through basic system functionality supported by formally documented and agreed procedures covering joiners, leavers and changes. Leavers and temporary staff are de-registered promptly.	Auditors require assurance that: • System reports and logs are enabled and adequately monitored. • System alert thresholds and control standards have been set in line with agreed policies (e.g. failed login lockout, inactivity timers, password rules, inactive accounts). • System authentication controls prevent access by unauthorised individuals. • Staff do not accrue access rights as they move between jobs or change duties, as removal of access on change of duties is often overlooked.	As level 1 plus: • System logs. • System administrator reports. • System security policy. • System security procedures (access controls). • Audit findings and reports. • User access forms (especially leavers and changes). • Relevant survey responses.

[I] Look out for system policies that are simply clones of each other which can lead to false perceptions of system risks and controls in place. Consistency is to be encouraged but policies must reflect the system for which they are written and not be too generic.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Access controls, processes and procedures are reviewed regularly. The Senior Information Risk Owner (SIRO) or equivalent is regularly briefed on this aspect of governance.	Auditors require assurance that: • Policies, procedures and processes governing access controls are regularly reviewed. • Changes to access controls and relevant policies/ procedures are clearly communicated to relevant staff and system users. • Security events and incidents relating to access control breaches are analysed and the learning is captured. • Learning identified is fed into reviews that lead to improvement. • SIRO reports on access controls are comprehensive and evidence based - covering both compliance and risk. • Findings from audits and any automated network/ system monitoring and testing are progressed to closure and implemented where appropriate.	As level 2 plus: • Evidence of documented and controlled change to relevant policies, processes, and procedures. • Changes signed off by email or other correspondence by authorised individual (e.g. SIRO) or delegated individual/ group. • Analysis of security incident reports. • Improvement or other action plans emanating from audit findings or other reviews. • Security reports and briefings for the SIRO.[l] • Minutes from relevant meetings or groups responsible for review of policies and procedures or progression of recommendations for improvement.

.

[l] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Information Security Assurance - SIRO Role (8307)

No.	IG Requirement
8307	An effectively supported Senior Information Risk Owner (SIRO) takes ownership of the organisation's information risk policy and information risk management strategy.

Objective of the requirement

66 A senior Board level or equivalent individual has been nominated as SIRO and is responsible for owning information risk in the organisation. The SIRO supports the Board and the Accounting Officer in terms of information risk and the organisational response.

Reference knowledge for auditors

67 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- Cabinet Office: Data Handling Procedures in Government: Final Report 2008
- DH: NHS IG - Information Risk Management: Good Practice Guide 2009
- DH: NHS Information Security Code of Practice 2007
- BSI: ISO/IEC 27000 Series of Information Security Standards

Table 21 Assurance required

Requirement 8307 - SIRO Role

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A Senior Information Risk Owner (SIRO) is in post with an effective support infrastructure. The SIRO has: • adequate information risk skills; and • adequate knowledge and experience to effectively coordinate and implement a programme of information risk management across the organisation.	Auditors require assurance that: • The SIRO is sufficiently senior in the organisation (Board level or equivalent). • The SIRO is suitably qualified[i] and experienced for the role. • The role is formally identified and given sufficient weight in the individual's job description (especially where SIRO duties form part of a wider full-time role). • A comprehensive and up to date information asset register is in place. • Information Asset Owners (IAOs) for key information assets have been identified.	• Nominated individual as SIRO in the IG Framework document. • Relevant Board minutes or relevant delegated group. • SIRO job description. • Evidence of appropriate support infrastructure, e.g. access to an accredited IT Security Professional - see req 8300. • SIRO continuing professional development (CPD) log. • Documented information asset register.[ii] • IAO details recorded against asset register details.

[i] For example, is already leading on risk management or information governance at Board level; has an understanding of how the strategic business goals of the organisation may be impacted by information risks, etc. Ensure that, where appropriate, any continuous professional development requirements are maintained and up to date.

[ii] This must have effective mechanisms and processes to maintain its currency, ideally linked to an ITIL compliant Configuration Management Database within a wider service management framework. Asset registers that are only right 'at a single moment in time' in order to satisfy the needs of the auditors are not credible as evidence of effective management and control of information assets.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	Staff comprising the support structure (Information Asset Owners - IAOs) are established in line with records in the information asset register. SIRO and IAOs have received suitable training. Key information assets have been risk assessed and are re-assessed on a cyclical basis.	Auditors require assurance that: • Training needs for SIRO and IAOs have been assessed and met. • Information assets have been categorised for risk and frequency of review.	As level 1 plus: • Documented training needs analysis. • Evidence of attendance. • Review of relevant training material. • Risk assessment frameworks for information assets that are documented: o consistently applied; and o in line with corporate risk management arrangements and methods. • Documented risk reviews for information assets and evidence of inclusion of findings in SIRO Board reports. • Documented action plans arising from information asset risk reviews.
3	Arrangements for information risk are reviewed regularly and the SIRO updates strategic information risk management training at least annually.[i]	Auditors require assurance that: • Documented reviews of arrangements have taken place and are informed by risk assessments and their findings. • Changes to arrangements are subject to documented formal approval by the Board or delegated group. • SIRO training is refreshed annually either through the NHS IG Training Tool or equivalent external training. • Reviews to training material take account of national policy changes as well as local feedback from past delegates.	As level 2 plus: • Review documents for information assets. • Board or other minutes approving changes. • Attendance records for training (internal and external). • SIRO CPD log. • Review of changes to relevant training material that includes the audit trail of the change.

[i] This may include elements of continuous professional development.

Information Security Assurance - Information Transfers (8308)

No.	IG Requirement
8308	All transfers of hard copy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.

Objective of the requirement

68 To achieve secure transfers of personal data.

69 Mapping data flows will help the organisation identify how personal identifiable information is transferred into and out of the organisation. More importantly, it will allow the organisation to assess risks and ensure staff are provided with clear procedures regarding the handling of personal information received.

Reference knowledge for auditors[i]

70 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- CQC: Essential Standards of Quality and Safety
- David Nicholson Communications
- DH: NHS Operating Framework for England for 2010/11
- DH: Informatics Planning 2010/11
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- DH: NHS IG - Short Message Service & Texting
- DH: NHS IG - Good Practice Guide - transfer of Batched Person Identifiable Data
- DH: NHS - IG Guidelines on Use of Encryption to Protect Personal Identifiable and Sensitive Information 2008
- DH: Caldicott Guardian Manual 2010
- DH: Information Security NHS Code of Practice 2007
- NIGB: NHS Care Record Guarantee (England)
- Information Mapping Tool Guidance
- BSI: ISO/IEC 27000 Series Information Security Standards

[i] Items marked (*) are accessible by NHS Network users only

Appendix 3 – 8300 Series

- NHS CFH: Good Practice Guidelines - Information Security *
- NHS CFH: NHS Encryption Tool

Table 22 Assurance required

Requirement 8308 - Information Transfers

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a documented and approved plan for securing digital and hardcopy transfers / flows of person identifiable and sensitive information in and out of the organisation.	Auditors require assurance that: • The organisation has developed relevant policies, procedures and plans for the movement of information into, around and out of the organisation. • The procedures have been developed and documented to clearly and unambiguously define the routine methods to be used for receiving and transferring key person-identifiable information.[I] • These procedures have been formally approved - Auditors must ensure that these policies, plans, and procedures apply equally to hardcopy and digital information and that their content is sufficiently robust and reflective of NHS guidance.	• Documented policies, procedures and plans. • Minutes of meetings at which such were approved. • Reference within policies, procedures and plans to relevant legislation and/or NHS guidance.
2	Routine transfers of person identifiable and sensitive information in all areas have been identified, mapped and risk assessed. All risks are appropriately recorded in the risk register along with the actions taken to secure the information. Information Asset Owners - IAOs (or equivalent) have developed information agreements and procedures to ensure transfers are adequately protected, comply with NHS	Auditors require assurance that: • All routine flows of person identifiable information[II] for the organisation have been identified and recorded. • Related risks have been assessed, recorded in the organisation's risk register and reported to the overseeing group (the Information Governance Steering Group or similar). • Significant risks have been reported to the	As level 1 plus: • Reports from the Information Mapping tool. • Documented description of the information flows that are routed through safe havens. • Risk Register, identifying risks to information flows. • Reports to, and minutes of, Information Governance Steering

[I] This relates to both patient and non-patient information

[II] The NHS definition of person identifiable data is more rigorous than that in the Data Protection Act 1998.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
	Codes of Practice and NHS IG standards and ensure their staff that transfer or receive this information are effectively informed of the procedure which applies to the transfer method they use.	Senior Information Risk Owner (SIRO); • Documented procedures for the secure transfer of data. • All procedures for the secure transfer of data have been approved by senior management, and implemented in the organisation. • The organisation has in place procedures to ensure that all relevant staff have been effectively informed of the secure transfer requirements for person identifiable and sensitive information, and have been made aware of the location of safe havens. This includes non-clinical staff such as switchboard operators and post room staff.	Group, considering risks to information flows. • Reports to the SIRO. • Records of senior management sign-off of secure transfer procedures. • Evidence that the procedures for secure transfers are available to staff at appropriate points in the organisation, accessible to staff, such as an intranet, or distribution to appropriate departments. • Published list of the types and locations of safe havens.
3	Information risk leads (SIRO and IAOs) routinely review information transfer policy, procedures and agreements, to ensure that the measures in use continue to be effective and to consider changes to the existing procedures and alternative methods of transfer. Monitoring arrangements exist to ensure compliance and effectiveness of policy and procedures.	Auditors require assurance that: • There is a regular review of documented policies to ensure that they remain appropriate. • There are regular reviews of the mapped and actual flows of person identifiable information, in and out of the organisation, resulting in updated secure transfer procedures and lists, and risk register if appropriate. • There is a process for notifying new flows of information, and updating secure transfer procedures and lists. • There are means to check the receipt of information at safe havens, and receipt of	As level 2 plus: • Policy/procedure review and approval. • Revised/previous mapped information flows. • Revised/previous secure transfer procedures. • Revised/previous list of safe haven locations. • Revised/previous risk register. • Job description including the task of monitoring the use of safe havens. • Automatic or manual logs of information received at safe havens. • Audit reports regarding compliance[i].

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		person identifiable information through other channels. These may be by spot checks, monitoring exercises to observe information inflows over a period, and/or by the use of records and logs, and by marking the origin of all received person identifiable information. • The organisation actively checks all inbound flows of person identifiable information, to ensure compliance with the secure transfer procedures, and to prevent any inappropriate use of safe havens for non-confidential information.	• Incident logs of confidential information received by inappropriate channels. • Surveys or spot checks on staff, to determine if they can identify secure transfer procedures and appropriate safe haven locations. • Surveys or spot checks of the use of safe havens. • Surveys or spot checks of the origin of person identifiable information, for example by letter, fax, email, magnetic or optical media. • Reports to, and minutes of, the committee examining the working of the secure transfer procedures and any information governance issues raised.

Information Security Assurance - Business Continuity (8309)

No.	IG Requirement
8309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and services - specific measures are in place.

Objective of the requirement

71 To counteract or minimise interruptions to business as usual as a result of major failure, disruption or disaster adversely affecting the organisation's information assets. This is an integral part of corporate risk management and emergency planning.

Reference knowledge for auditors[l]

72 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Good Practice Guide for the Transfer of Batched Person Identifiable Data
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- DH: NHS Resilience Resources Incorporating the BS25999 Standard
- NHS CFH: Good Practice Guidelines - Business Continuity and Disaster Planning *
- Business Continuity Institute : Good Practice Guidelines
- Business Continuity Manual 2003
- BSI: ISO/IEC 27000 Series Information Security Standards
- BSI NHS 25999-1 2009 Business Continuity Management for the NHS

[l] Items marked (*) are accessible by NHS Network users only

Table 23 Assurance required

Requirement 8309 - Business Continuity

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	The Senior Information Risk Owner (SIRO) is leading the organisational approach which incorporates Information Asset Owner (IAO) responsibilities and has the support and involvement of senior management. The SIRO has ensured that all business critical systems have been identified (including externally managed systems). IAOs understand their responsibility for analysing the business functions that their systems support. IAOs understand their responsibility to assess the impact of potential disruption and form plans for each asset that facilitate a controlled return to business as usual.	Auditors require assurance that: • A SIRO led strategy for business continuity exists that covers the whole organisation; supported by a programme with nominated responsibilities and overall approach. • Senior management have approved the business continuity strategy, programme and overall approach. • All critical systems have been identified, assessed and mapped to their associated business function. • Business function analysis links to the development of an effective and credible recovery plan can be drawn up for both the business function and its attendant systems.	• Documented business continuity strategy. • Evidence of senior management approval. • Mapping of critical information assets to business functions. • A record of existing business continuity documents in the information asset register.[I]
2	Approved and documented plans are in place for all critical information assets. Staff are aware of roles and responsibilities. Procedures and controls for backup and recovery of critical information assets assure their integrity and availability.	Auditors require assurance that: • Business function analysis has been completed for all key systems; risks are managed as part of the corporate risk management approach. • Business continuity plans are in place for all critical information assets; these have documented SIRO approval.	As level 1 plus • Corporate risk register. • Documented evidence of business function analysis.[II] • Documented and SIRO approved business continuity plans. • Evidence of staff awareness e.g. briefings, training material or minutes

[I] Business continuity plans and associated documents are key information assets in their own right. Investigations of past incidents have sometimes found that the management, control and accessibility of plans and associated documentation is overlooked.
[II] This may reasonably be integrated into business continuity plans.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		• Staff understand key essentials of business continuity plans as these affect their role. • Procedures for controlled shut down, back-up and recovery of critical information assets are in place and form part of system level security policies.	from meetings. • System level security policies[I] that cover system specific details of backup and recovery plans.
3	Overall business continuity plans are tested to ensure they are credible, feasible, practical and reliable. Tests may be partial and constitute walk-through, table top, MAJAX tests or a combination of these. Specific controls are reviewed by IAOs following lessons learned from testing, audit and review. Business continuity plans, procedures and control measures are reviewed regularly in the light of new threats, changes in key personnel or arrangements, following major structural change, or in the absence of these; after a reasonable period of time[II].	Auditors require assurance that: • Testing is documented and recorded through minutes, agendas and other records that capture learning from the event. • System procedures, policies and controls are changed to take account of audit findings, test results and other operational learning processes. • Changes to procedures are documented and approved and are not made in isolation but are integrated into wider business continuity arrangements.	As level 2 plus • Audit reports for specific systems. • Documented review of testing[III]. • Formal approval of changes to business continuity plans, procedures or controls. • Test plans. • Recovery test records and other test results. • Routine documented checks and maintenance on critical failsafe devices such as uninterruptible power supply (UPS).

[I] Auditors should look out for cloned security policies and in particular cut and paste of details such as the availability and specification of UPS equipment or the back up hierarchy in place; these may differ across systems.

[II] Accepted good practice is that a formal review should be carried out at least annually.

[III] Auditors should be mindful that continuity plan testing should drive out any inconsistencies or deficiencies in the plans. It is not uncommon, therefore, for tests to "fail". Where this is the case auditors must be wary of supporting a level three score as such a score "implies" that there is a robust approach upon which the organisation can place assurance.

Information Security Assurance - Processing Disruption (8310)

No.	IG Requirement
8310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.

Objective of the requirement

73 Equipment must be protected to prevent the compromise of information assets. Threats include infrastructure failure, equipment failure, environmental hazard, one off incidents or disasters and human error. Special consideration must be given to the protection of mobile equipment - see also requirement 8314.

Reference knowledge for auditors

74 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: NHS Resilience Resources Incorporating the BS25999 Standard
- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- DH: NHS IG - Good Practice Guide for the Transfer of Batched Person Identifiable Data
- BSI: ISO/IEC 27000 Series Information Security Standards

Table 24 Assurance required

Requirement 8310 - Processing Disruption

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Information Asset Owners (IAOs) are responsible for establishing appropriate documented procedures and effective controls to protect their information assets from equipment failure, environmental hazard and human error.	Auditors require assurance that: • Procedures and requirements are based on comprehensive and up to date risk assessments. (Req. 8301). • Procedures and requirements fully address equipment failure, environmental hazard and human error risks. • Procedures and requirements have been approved by SIRO or IAOs.	• System level security policies[I]. • Outputs from the risk assessment completed under Req 8301. • Documented approval of procedures and controls by SIRO or IAOs. • Minutes of meetings.
2	IAOs establish and implement planned procedures and controls to mitigate against processing disruption risks.	Auditors require assurance that: • Protection exists through implementation of planned procedures and controls.	As level 1 plus • A documented report to appropriate senior manager or committee.
3	IAOs, or equivalent, monitor compliance with procedures and controls, as a basis for assuring the SIRO on the protection of information assets. Procedures and controls are reviewed in light of operational learning; changes are approved, documented and effectively communicated to relevant staff.	Auditors require assurance that: • Compliance monitoring is established. • Outcomes from compliance monitoring drive reviews of procedures and controls. • Security procedures and controls are an integral part of project initiation and business case for new information assets (Req. 8210). • Security procedures and controls are reviewed annually against new threats and developments in counter-measures.	As level 2 plus • Audit reports and outcomes from compliance checks.[I] • Key performance indicators (KPIs), for example, system availability. • Evidence of changes to security procedures and controls with documented approval of SIRO/ IAOs. • Business cases for new information assets (or corporate project templates and local guidance). • Review of system security policies.

[I] Auditors should look out for cloned security policies and in particular the generic mitigation of risks across systems. Consistency of approach is important and some common risks will be apparent but policies must reflect the system risk assessment.

Information Security Assurance - Malicious Code (8311)

No.	IG Requirement
8311	Information assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.

Objective of the requirement

75 Prevention or detection of the introduction of malicious and mobile code (viruses and malware) into the computer components of an organisation's information assets.

76 Viruses and malware have the potential to significantly damage business capability and impact on services and patients.

Reference knowledge for auditors[II]

77 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management: Good Practice Guide 2009
- NHS CFH: Good Practice Guidelines - Application Security *
- BSI: ISO/IEC 27000 Series Information Security Standards

[I] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

[II] Items marked (*) are accessible by NHS Network users only

Table 25 Assurance required

Requirement 8311 - Malicious Code

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Information assets have been risk-assessed for vulnerability to malicious and mobile code. Documented procedures exist to rapidly detect, isolate and remove such code.	Auditors require assurance that: • All information assets in the asset register (Req. 8307) have been assessed for risk. • Appropriate controls and procedures have been documented and approved; this has been done for each information asset.	• Asset register. • Documented risk assessments.[I] • Documented evidence of controls and procedures.
2	Approved and documented controls against malicious code have been fully implemented across the organisation for all information assets.	Auditors require assurance that: • Controls are implemented for all information assets. • New and changed requirements undergo an approval process (by Information Asset Owner or nominated System Administrator) to ensure risks against malicious code are minimised.[II]	As level 1 plus • Activity logs from control software (includes scanning, detection, removal and update of key software components). • Change management policy or procedures. • Minutes of information governance groups considering new or changes procedures. • Evidence of Project Management practice for implementing new

[I] This may form part of a wider system risk assessment completed under Req 8307

[II] This is also part of Req. 8210 on Information Asset Security Compliance

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			processes and information assets.
3	Information assets are routinely reviewed to ensure implemented controls are working to specification[i]. Alerts are proactively monitored and investigated.	Auditors require assurance that: • Controls are routinely reviewed for all information assets. • Procedures are being followed. • Incidents are caught early and dealt with swiftly. • Control software is configured to be always active, always up to date and outside the users control (i.e. users cannot disable it). • Supplier contracts for control software include updates and patches and licences have not expired.	As level 2 plus • System logs and activity reports. • Incident reports (relating to malicious code). • KPI's regarding, for example, number of outbreaks etc. • Minutes of meetings documenting review of procedures and controls. • Evidence of changes applied based on learning from incidents or reviews. • Documented and approved security policy, relevant to control software installation and configuration. • Information asset register (control software licences and contracts).

[i] In order to be fully effective, controls against malicious code must be right up to date and must be locked down so the user cannot disable them from the desktop or mobile device.

Information Security Assurance - Network Security (8313)

No.	IG Requirement
8313	Policy and procedures are in place to ensure that information communication technology (ICT) networks operate securely.

Objective of the requirement

78 Information communicated over networks must be appropriately secured, the supporting infrastructure must also be appropriately protected; this includes both wired and wireless networking.

Reference knowledge for auditors[I]

79 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- NHS CFH: Good Practice Guidelines in Information Governance - Information Security *
- BSI: ISO/IEC 27000 Series of Information Security Standards

[I] Items marked (*) are accessible by NHS Network users only

Table 26 Assurance required

Requirement 8313 - Network Security

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Networks have been risk-assessed by Information Asset Owners (IAOs) or nominated network administrator(s). Responsibility for network security has been assigned. Procedures, controls and operational responsibilities have been identified, documented and approved.	Auditors require assurance that: • Each network has an appropriate, Senior Information Risk Owner (SIRO) approved, security policy. • IAOs or nominated network administrators review network risks and identify controls and procedures required to mitigate risks. • Controls and procedures are approved by the SIRO or equivalent nominated individual or group.	• Network level security policies.[i] • Job description for network administrators. • Documented SIRO or delegated approval of policies, procedures, controls and responsibilities. • Network risk assessments (including mitigation).
2	Approved procedures and controls have been implemented for all networks.	Auditors require assurance that: • Controls have been implemented across all networks, in line with their respective network level security policies. • Procedures are available at appropriate parts of the organisation and can be accessed by relevant staff. • Staff understand the need for compliance and have been adequately briefed. • Staff requiring reasonable adjustments[i] have been appropriately catered for.	As level 1 plus • Integrated documented procedures and controls that include as examples: o security; o firewalls; o capacity plans; o gateways and domains; o file storage; o access rights (group and individual). • Staff guidance and procedures on the intranet. • Awareness and briefing materials for staff. • Inclusion in training material (including

[i] As for system level security policies, auditors should look out for generic 'cut and paste' security policies. A consistent approach is fine and while many elements of security policies for networks will be the same, security policies must reflect the relevant network risk assessment.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			induction).
3	Compliance is monitored; events and incidents result in swift remedial action. Networks are routinely reviewed for assurance reports to the SIRO.	Auditors require assurance that: • Compliance is monitored and exposures identified are addressed swiftly. • The SIRO receives regular assurance on network risks and overall compliance. • Policies, procedures and controls undergo regular review.	As level 2 plus • Outcomes of spot checks. • Audit reports and action plans (network management)[ii]. • Outcomes from technical reviews and penetration testing. • System alerts and logs. • Security incidents (related to networks). • SIRO assurance reports. • Documented approved and controlled changes to policies, procedures and controls linked to learning outcomes from checks, incidents and reviews. • Guidance for staff - has this been updated in line with changes to policies, procedures and controls.

[i] For example scalable fonts, large print, Braille or web content that can be used by a screen reader.

[ii] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Information Security Assurance - Mobile Security (8314)

No.	IG Requirement
8314	Policy and procedures ensure that mobile computing and teleworking are secure

Objective of the requirement

80 This is a major risk area. Risks include loss, damage and theft leading to inappropriate disclosure of information. Countermeasures must reflect risks that mobile and teleworking present.

Reference knowledge for auditors[I]

81 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- David Nicholson Communications
- DH: NHS IG - Good Practice Guide for the Transfer of Batched Person Identifiable Data
- NHS CFH: NHS Encryption Tool
- NHS CFH: Guidance on the Implementation of Encryption within NHS Organisations *
- BSI: ISO/IEC 27000 Series of Information Security Standards

[I] Items marked (*) are accessible by NHS Network users only

Table 27 Assurance required

Requirement 8314 - Mobile Security

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	All mobile and teleworking arrangements are subject to approval and authorisation by the relevant Information Asset Owner (IAO). Approvals are in line with a documented policy and supported by procedures including guidance for staff operating such working arrangements.	Auditors require assurance that: • Policy and procedures are in place. • Suitable guidance for staff has been developed and is readily available. • Policy and procedures have been approved by senior management.	• A documented and approved mobile security policy. • Relevant survey responses. • Record of approval of policy and procedures.
2	All mobile and teleworkers are approved and authorised. All such staff are aware of relevant guidance and procedures.[I] Suitable solutions and functionality are deployed for mobile devices and removable media to protect and secure them.	Auditors require assurance that: • Staff have seen, understood and agreed to comply with procedures. • Approval and authorisation is sought in advance of issue of mobile devices in all cases. • Approvals are not left open-ended but are rescinded and renewed in line with approved procedures; commensurate with business needs. • Robust remote access solutions are in place.[II]	As level 1 plus • Records of authorised/ approved use (including revocations).[III] • Relevant section of staff handbook. • Procedures (including staff guidance), available via intranet. • Briefing and awareness material. • Specification for remote access solution. • Audit trails and other system reports from remote access monitoring.

[I] It is recognised good practice to issue full or summarised staff procedures routinely with every mobile device; staff sign a statement of compliance to agree them as a condition of use.

[II] While this requirement focuses upon the technology of remote working auditors must be mindful of the variety of "side issues". For example; Where home workers have personally identifiable hard copy information in transit or at home is this adequately secured and assured? If there is secure remote access but this can be from any internet computer how is the security assured, e.g. to a home computer?

[III] Auditors should check a sample for excessively long-term or open-ended arrangements and also ensure that approvals pre-date loan arrangements.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	Mobile and teleworking arrangements are regularly reviewed, audited and monitored for compliance. Non-compliance is identified and results in swift action to address exposures.	Auditors require assurance that: • Procedures have been understood and are being followed by staff. • Mobile arrangements are only in place for authorised users. • Mobile devices are all accounted for and sensitive or personal information stored on them is encrypted in line with NHS and National minimum standards.[i] • Policy and procedures on mobile working arrangements are subject to periodic review.	As level 2 plus • Outcomes of spot checks. • Audit reports and action plans (mobile working arrangements). • Outcomes from technical reviews (remote access and encryption). • Remote access system alerts and logs. • Security incidents (related to mobile security). • Technical specification for encryption. • Documented approved and controlled changes to policies, procedures and guidance linked to learning outcomes from checks, incidents and reviews. • Guidance for staff - has this been updated in line with changes to policies and procedures.

[i] National minimum guidance on encryption is that this must meet the FIPS 140-2 standard. NHS provides separate standards on encryption and access to the NHS Encryption Tool.

Information Security Assurance - Airwave Security (8315)

No.	IG Requirement
8315	Security management requirements to protect the Airwave communications service are satisfied.

Objective of the requirement

82 To ensure that Airwave corporate information security responsibility, standards and policies are complied with by all users of the service.

Reference knowledge for auditors

83 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Information Security NHS Code of Practice 2007
- BSI: ISO/IEC 27000 Series of Information Security Standards
- DH NHS IG - Information Risk Management: Good Practice Guide 2009

Table 28 Assurance required

Requirement 8315 - Airwave Security

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Responsibility for Airwave has been assigned and a plan to meet service connection requirements and standards is in place.	Auditors require assurance that: • A senior reporting officer has been appointed. • An appropriate documented plan has been developed to meet the code of practice	• Job description or other documented evidence of appointment. • Implementation plan and supporting evidence of action taken or required.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		requirements.	
2	Measures to comply with the requirements of the Airwave (NHS) code of practice have been implemented.	Auditors require assurance that: • Physical security requirements are met. • Accreditation Document Set (ADS) standards have been met. • Code of Connection (appendices A and C) requirements are met. • There is effective and compliant incident reporting and management arrangements for Airwave that interface and integrate with overall incident management processes, risk assessments and wider business continuity arrangements.	As level 1 plus: • Reports from audits of physical security and outcomes from compliance checks on server rooms. • Entry control system logs including lists of authorised personnel. • Documented authorisation for access (including revocations). • Regular changes to secure entry systems, particularly following changes to authorised personnel.[i] • Updated plans showing action taken to meet code and accreditation standards. • Documented sign-off of by senior management of implementation. • Integration of Airwave arrangements in overall business continuity plans (Req. 8309), incident reporting arrangements (Req 8302) and risk assessments (Reqs 8210 and 8301).
3	Standards and practice are reviewed on a regular basis.	Auditors require assurance that: • An ongoing dialogue exists between the organisation and the Ambulance Radio Programme (ARP) with regard to incidents and exposures. • Compliance is monitored and exposures identified are addressed swiftly. • The Airwave provision is subject to regular audit.	As level 2 plus • Correspondence between the organisation and the ARP and minutes from meetings. • Minutes from the ARP Working Group (six monthly) showing regularity and continuity of attendance. • Outcomes of spot checks. • Audit reports and action plans

[i] It is recognised good practice to change shared access codes (e.g. keypad code) on a regular basis and immediately following any removal of authorised users.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
		- Airwave standards and practice undergo regular review by a senior IG group.	(Airwave)[i]. - System alerts and logs. - Security incidents (related to Airwave). - Documented approved and controlled changes to policies, procedures and controls linked to learning outcomes from checks, incidents and reviews.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Information Security Assurance - Organisational and Technical Measures (8323)

No.	IG Requirement
8323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.

Objective of the requirement

84 All information assets that hold or are personal data must be protected by organisational and technical measures. Measures should reflect the nature of the asset, the sensitivity of the data and be commensurate with the overall risk.

Reference knowledge for auditors[I]

85 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH NHS IG - Information Risk Management: Good Practice Guide 2009
- DH: Information Security NHS Code of Practice 2007
- DH: NHS IG - Guidance for the Classification Marking of NHS Information 2009
- NHS CFH: Good Practice Guidelines - Application Security *
- NHS CFH: Good Practice Guidelines - Disposal and Destruction of Sensitive Data *
- NHS CFH: Good Practice Guidelines - Web Server Security *
- NHS CFH: Good Practice Guidelines - Securing Web Infrastructure and Supporting Services *
- BSI: ISO/IEC 27000 Series of Information Security Standards
- BSI: ISO/IEC 20000-2:2005 Information Technology Service Management Code of Practice

[I] Items marked (*) are accessible by NHS Network users only

Table 29 Assurance required

Requirement 8323 - Organisational and Technical Measures

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Information assets that are or hold personal data appear in the information asset register and have a clearly identifiable Information Asset Owner (IAO).	Auditors require assurance that: • The information asset register includes all identified assets[I] that hold personal data. • Every recorded information asset has a nominated IAO. • A documented plan is in place to assess all remaining information assets and identify those that hold or comprise personal data and bring these within the scope of the asset register and assign a suitable nominated IAO.	• Documented information asset register. • Documented action plan to review all remaining information assets.[II]
2	Mandatory safeguards are in place to protect assets that hold or comprise personal data. Further risks assessments have been undertaken to determine the need for any additional safeguards. The plan to identify any previous unknown information assets has been implemented, the organisation is confident that all such assets have been identified, documented	Auditors require assurance that: • Mandatory safeguards have been deployed. • Additional risk assessments are complete • All information assets have been identified and assessed.	As level 1 plus • Information on the status of mandatory safeguards. • Information asset risk reviews and details of additional safeguards - included as part of information asset register records. • Report to senior management on the status of information asset risk.

[I] The auditor interpretation of this is that where an asset has been identified as comprising or holding personal data, it must be included in the information asset register. However' level 1 compliance recognises that there may be additional assets, yet to be identified, that comprise or hold personal data. These are picked up at level 2 of the requirement.

[II] This may link to system risk assessments undertaken as part of Req. 8301

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
	and assigned to IAOs.		
3	All personal data information assets are appropriately secured. Compliance with policies and procedures is monitored. New and changed systems are captured, risk assessed, documented and assigned. Procedures are reviewed in line with revised new working practices, new risks and improved technical safeguards.	Auditors require assurance that: • All discretionary (additional) safeguards have been deployed. • Audits and spot checks are carried out • Learning is identified and captured. • Changes and improvements reflect audit outcomes. • New and changed information assets will automatically be captured, risk assessed and documented as an information asset. • Procedures are subject to regular review, controlled change and sign-off.	As level 2 plus • Audit and spot check reports (with findings and recommendations).[i] • Schedule of compliance checks. • Project templates and change management procedures for new and changed information assets ensure privacy impact assessments and asset register details are completed. • Documented instruction to IAOs to ensure awareness, agreement and effective operation of procedure for new and changed assets. • Documented approved and controlled changes to policies, procedures and safeguards linked to learning outcomes from checks, incidents and reviews.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the 'picture painted' by level 2 or 3 compliance.

Information Security Assurance - Pseudonymisation and Anonymisation (8324)

No.	IG Requirement
8324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate.

Objective of the requirement

86 To ensure that only the minimum personal data required to satisfy a purpose is collected and used and unnecessary information is stripped out. This meets fundamental Data Protection Act 1998 principles as well as Caldicott principles and the Human Rights Act 1998.

Reference knowledge for auditors

87 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- ISO/TS 25237:2008 - Health Informatics Pseudonymisation
- NHS CFH: Pseudonymisation Implementation Project - Guidance on Terminology
- NHS CFH: Pseudonymisation Implementation Project - Guidance on De-identification
- NHS CFH: Pseudonymisation Implementation Project - Guidance on Business Processes and New Safe Havens
- NHS CFH: Pseudonymisation Implementation Project - Guidance on Local NHS Data Usage and Governance for Secondary Uses
- DH: Confidentiality NHS Code of Practice 2003
- DH: The Caldicott Guardian Manual 2010
- National IG Board: The NHS Care Record Guarantee for England

Table 30 Assurance required

Requirement 8324 - Pseudonymisation and Anonymisation

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	A plan exists to protect the confidentiality of service user information through pseudonymisation and anonymisation of information (other than where this used for direct care purposes).	Auditors require assurance that: • A plan is in development. • The plan reflects current DH guidance. • The plan is signed off by senior management. • A nominated individual or group is assigned responsibility for the plan.	• A documented implementation plan is under development or in place. • Job description or terms of reference that include the implementation of pseudonymisation and anonymisation. • Documented evidence of Board level or senior management sign-off.
2	The implementation of pseudonymisation and anonymisation is supported by effective information governance. The planned business process change has been implemented in full.	Auditors require assurance that: • The organisation has attained level 2 for all key requirements within the Information Governance Management, Confidentiality and Data Protection and Information Security Assurance sections of the Information Governance Toolkit (8100, 8200 and 8300 series). • All secondary use services that require pseudonymisation and anonymisation of data are compliant. • Safe haven processes that meet DH guidance are in place.	As level 1 plus • Completed IGT assessment. • Project plans and project level documentation.[l]

[l] Such is the potential impact across a range of business processes that most organisations will implement this as a project, auditors should expect to be able to reference appropriate project plans and other associated documentation. However there will be exceptions to this approach in which case alternative evidence will be required.

Appendix 3 – 8300 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	In order to remain compliant, regular review of business processes is necessary to maintain service user confidentiality.	Auditors require assurance that: • The effectiveness of pseudonymisation and anonymisation business processes and functions are subject to annual external audit. • Business processes are subject to regular review, controlled change and sign-off.	As level 2 plus • External audit report.[i] • Documented approved and controlled changes to business processes linked to learning outcomes from reviews.

[i] Note: while the IG Toolkit only requires that the organisation has monitoring/audit processes in place with feedback to professionals, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives this would contradict the ‘picture painted’ by level 2 or 3 compliance.

Appendix 4 – 8400 Series

Clinical Information Assurance - Skills and Experience (8400)

No.	IG Requirement
8400	The information governance agenda is supported by adequate information quality and records management skills, knowledge and experience.

Objective of the requirement

88 Sufficient skills knowledge and experience are in place to support information quality and records management assurance covering both health and corporate records for the entire organisation. Competence levels should be linked to duties and responsibilities and not generically defined.

Reference knowledge for auditors

89 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: Records Management NHS Code of Practice 2006
- DH: Records Management Roadmap

Table 31 Assurance required

Requirement 8400 - Skills and Experience

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	Information quality and records manager or officer roles are assigned to suitably qualified and skilled individuals with an approved plan and resources in place covering information quality and records management.	Auditors require assurance that: • A suitably qualified information quality and records manager or officer has been assigned. • A plan to identify information quality and records management work has been developed and endorsed by senior management. • Additional information quality and records assurance resources have been identified or established. • Appropriate information quality and records	• Named job description or formal assignment of responsibility. • A clear and detailed plan for the development of an information quality and records management framework, where none exists. This should include named resources, timescales, milestones and dependencies. • Minutes or meeting papers documenting the assignment of responsibility and approval of the plan. • Evidence of professional qualifications and/ or membership of relevant professional bodies.[l]
2	An information quality and records management framework in place together with the skills, knowledge, experience and resources to deliver it (including specialist external functions). Responsibility is identified and documented across a range of staff roles.	Auditors require assurance that: • An effective information quality and records management function is established. • Staff with specialist information quality and records management roles have been fully trained. • The information quality and records management work programme is established and underway. • Specialist resources are available as required (these may be shared resources between organisations).	As level 1 plus • Training records for specialist and key staff. • Relevant survey responses. • Service level or other documented agreements with providers of specialist resources. • Policies, strategies, improvement plans, logs and reports arising from the work of the information quality and records management function.

[l] Ensure that, where appropriate, any continuous professional development requirements are maintained and up to date

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	The work programme for the information quality and records management function is integrated as part of overall IG work, formally approved and regularly reviewed which drives improvement.	Auditors require assurance that: • The information quality and records management work programme forms an integrated part of the wider corporate risk arrangements. • The senior nominated IG Forum or Board formally approve the work done which contributes to the annual IG improvement plan. • Information quality and records management arrangements are reviewed annually for alignment with advances in technology as well as changes in legislation and guidance. • Learning and action from review is identified and leads to controlled change to information quality and records management arrangements.	As level 2 plus • Clear links between the plan for the information quality and records management work programme and the corporate IG plan. The plan is monitored to ensure effective implementation. • Minutes of other meeting papers from the Board or delegated group reviewing and approving work done by the information quality and records management function. • Application of learning outcomes from reviews of the information quality and records management programme. • Evidence of controlled change to information quality and records management arrangements. • Evidence of planned review against technological developments, changes to national guidance and relevant legislation.

Clinical Information Assurance - NHS Number (8401)

No.	IG Requirement
8401	There is consistent and comprehensive use of the NHS Number in line with NPSA requirements.

Objective of the requirement

90 The organisation is assured of the consistent and comprehensive use of the NHS Number.

91 The NHS Number is the only national unique patient identifier in operation in the NHS. Using the NHS Number makes it possible to share patient information safely, efficiently and accurately across NHS organisations.

Reference knowledge for auditors

92 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- NHS Information Standards Board: NHS Number Information Standard for Secondary Care
- NPSA: Safer Practice Notice for the NHS Number
- NHS CFH: Implementation Guidance to Support the Adoption of NHS Number Standards
- NHS CFH: NHS Number Communication Toolkit
- DH: NHS Operating Framework for England 2010/11

Table 32 Assurance required

Requirement 8401 - NHS Number

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a project plan in place to support the consistent and comprehensive use of NHS Number.	Auditors require assurance that: • The organisation has in place robust plans to implement the use of the NHS Number including both system and people elements.	• System level reports describing whether they can support the NHS Number and what actions are required to facilitate this. • Clarity of roles and responsibilities within the project (job descriptions etc). • Project initiation document including objectives, risks, roles (boards, project staff etc), benefits plan etc. • Project plan setting out: o Business change process; o System implications and activities; o Training and other human issues; o Responsible Owners; o People that need to be involved; o Deadlines and dates (including those relating to system suppliers); o Dependencies; o Risks and issues (not just project risk but also wider impact risks); o Communications plan. • Evidence of approval of the plan (e.g. Trust Board or Project Board minutes). • Evidence of communication with staff such as Team Brief, newsletters etc. • Evidence of clear risk reporting and management plans such as risk registers, project board meeting

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			minutes, inclusion in corporate risk approach (note this is a key issue as the project should not be delivered in isolation of corporate risk.
2	Progress is being made, and any issues outside the control of the organisation are understood and being managed.	Auditors require assurance that: • The project is being effectively managed and delivered and that associated risks and issues are understood and managed appropriately.	As level 1 plus • Evidence of regular project progress reporting including: o Progress against timelines and budget (milestone reports); o Risk and issue logs and management plans[i]; o Project assurance reports.
3	The project outcomes have been documented and local governance has agreed closure of the NHS Number project.	Auditors require assurance that: • The project been delivered and formally closed. • A process has been established to ensure that all new systems are able to comply with the NHS Number requirement (ensuring on-going compliance).	As level 2 plus • There should be a formal project closure report setting out the original objectives and milestones and the “closed” position. • Any outstanding actions and risks/issues should be formally documented and processes should be established to ensure that these are delivered, managed and reported in the absence of the project board. • The report should be presented to and approved by the project board – this should be evidenced in minutes. • The closure report, or a similar accompanying document, should set out the process by which future systems will be assessed and assured.

[i] Note: it is not sufficient to have risks and issues logged, they must be assigned and there must be evidence of ownership and action planning.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			• If any new systems have been implemented since the project closure auditors should review the project documents for such system implementations in order to ensure that the requirements have been considered and acted upon.

Clinical Information Assurance - Accuracy of Care Records (8402)

No.	IG Requirement
8402	Procedures are in place to ensure the accuracy of service user information on all systems and/ or care records that support the provision of care.

Objective of the requirement

93 Effective procedures should be in place to ensure the accuracy of service user information.

94 Staff must be provided with procedures for collecting and accurately recording service user information on key operational systems, and routinely checking information with the source. The procedures must be monitored and where errors are identified, for example duplicate or confused records, corrections should be made.

Reference knowledge for auditors

95 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH: EL (97) 47 - Managing Data Quality Improvements and Data Accreditation
- NHS Information Standards Board: Information Standards Notice (ISN)
- DH: Measuring and Recording Waiting Times 2002
- Data Protection Act 1998
- DH: NHS Operating Framework for England 2010/11

Table 33 Assurance required

Requirement 8402 - Accuracy of Care Records

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are documented and approved procedures to ensure the accuracy of service user information on all key operational systems which include the collection and recording of accurate and complete information, validation of data and processes to identify and correct errors and omission. A training programme (including assessment of needs) has been developed to ensure staff members accurately collect and record service user information and routinely check information with an appropriate source.	Auditors require assurance that: • The organisation has developed, approved and disseminated robust procedures that are based upon latest NHS guidance. • Training needs have been assessed to ensure that staff are supported to accurately collect and record service user information and routinely check information with an appropriate source. • The training programme includes appropriate training materials and a roll out plan which ensures that all relevant staff will be trained within an acceptable/appropriate timeframe.	• Job descriptions setting out roles and responsibilities for the development and maintenance of related policies and procedures. • Policies and procedures that have been based on NHS guidance. • Evidence of approval of the policies and procedures, e.g. minutes, in accordance with organisational approval processes. • Evidence that policies and procedures have been subject to review and maintenance in accordance with review timetables (or where these do not exist within a reasonable time period e.g. annually). • Training materials are based upon approved procedures. • A training needs assessment that identifies the individuals and staff groups that require training.
2	The documented procedures have been implemented and made available to relevant staff. All staff collecting and recording data are effectively trained to do so and to take appropriate action where errors and omissions are identified.	Auditors require assurance that: • Relevant staff have received the training and that they have understood the content, and how this is to be applied, and reconciliation procedures are being routinely applied.	As level 1 plus: • Evidence that procedures are available to all relevant staff (intranet etc). • Training records etc demonstrating that individuals have attended training. • Evidence that the roles and responsibilities for such individuals are included in job descriptions.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
	Dedicated staff carry out activity reconciliations between the service user record and data held on key systems and the correction of any errors and omissions.		• Relevant survey responses. • Records of reconciliations, signed and dated, that identify discrepancies and corrective action – check that such corrections have been made. • Discussions with staff to ascertain operational procedures and comparison of these to documented procedures (looking for differences).
3	Data collection activities are monitored and routinely audited for effectiveness.	Auditors require assurance that: • The organisation has processes in place to monitor and audit the application and effectiveness of its procedures. • The outcome of this monitoring and audit provides assurance to the organisation that procedures are adequate.[I]	As level 2 plus: • Key performance indicators have been established and are monitored (e.g. for data accuracy). • Evidence that the organisation has, through internal or independent monitoring, received assurance that procedures are being routinely applied and are achieving the desired outcomes. • Evidence that any opportunities for improvement are captured in action plans and the implementation is monitored to ensure completion.

[I] Note: while the IG Toolkit only requires that the organisation has monitoring and audit processes in place. Auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify a failure to apply procedures or a failure to achieve objectives, this would contradict the ‘picture painted’ by level 3 compliance. Where this is the case, the validity of a level 2 score may also be questioned if evidence from monitoring indicates that the application of processes required for level 2 is not being met.

Clinical Information Assurance - Cross Specialty Clinical Records Audit (8404)

No.	IG Requirement
8404	A multi-professional audit of clinical records across all specialties has been undertaken.

Objective of the requirement

96 The organisation is assured of the quality of the health record.

97 It is essential that organisations undertake audits of clinical/care record keeping in all specialties to ensure that the quality of the health or social care record facilitates high quality treatment and care and that subsequently a health or social care record can justify any decisions taken if required. The NHS Litigation Authority, in particular, require organisations, especially those providing Maternity services, to demonstrate evidence of clinical records audits in the period prior to NHSLA Risk Management assessment.

Reference knowledge for auditors

98 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- DH Records Management NHS Code of Practice 2006
- CQC: Essential Standards of Quality and Safety
- NHS Litigation Authority: Risk Management Standards
- Royal College of Physicians: Generic Record Keeping Standards
- NHS Information Standards Board: Health Record and Communication Practice Standards

Table 34 Assurance required

Requirement 8404 - Cross-Specialty Clinical Records Audit

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There is a documented strategy for auditing clinical/care record keeping standards.	Auditors require assurance that: • The organisation has developed, approved and disseminated a robust strategy based upon latest NHS guidance.	• Job descriptions, or similar communication, setting out roles and responsibilities for the development and maintenance of related strategies, policies and procedures. • Strategies, policies and procedures that have been based on NHS guidance. • Evidence of approval of above, e.g. minutes, in accordance with organisational approval processes. • Evidence that policies and procedures have been subject to review and maintenance in accordance with review timetables (or where these do not exist, within a reasonable time period e.g. annually). • Training materials based upon approved procedures. • A training needs assessment that identifies the individuals and staff groups that require training.

Appendix 4 – 8400 Series

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
2	The strategy has been implemented and all staff are effectively informed of their responsibilities with regards to record keeping.	Auditors require assurance that: • All staff are informed of their responsibilities and this is supported by appropriate training. • The strategy is available to all relevant staff and processes must be in place to turn strategy into practice; and • Record keeping audits are undertaken in accordance with the strategy and the organisation is receiving positive assurances regarding compliance.[i]	As level 1 plus: • Evidence that procedures etc are available to all relevant staff (intranet etc). • Training records etc demonstrating that individuals have attended training. • Evidence that the roles and responsibilities for such individuals are included in job descriptions / objectives / KSFs[ii] etc. • Feedback from staff, e.g. through a survey, regarding whether they have received training. • Discussions with staff to ascertain operational procedures and comparison of these to documented procedures (looking for differences). • Positive assurances and outcomes from audit reports of record keeping standards (covering all professional groups and at least 50% of specialties). • Sample review of records to ensure compliance with agreed standards.

[i] Note: The IG Toolkit only requires that the organisation has monitoring and audit processes in place with feedback to professionals. Auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify a failure to apply procedures or failure to achieve objectives, this would contradict the 'picture painted' by level 2 or 3 compliance.

[ii] KSF – Key Skills Framework

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
3	An audit of record keeping standards has been completed for professional groups across all specialities (including maternity services where these are provided) with audit results being fed back to healthcare professionals. The strategy and training programme should be regularly reviewed and amended as appropriate.	Auditors require assurance that: • The organisation has in place processes to audit the application and effectiveness of its strategy and procedures. • The outcome of this audit provides assurance to the organisation that its strategy and procedures are adequate and are being routinely applied.	As level 2 plus: • Key performance indicators have been established and are monitored (e.g. for data accuracy). • Outcomes from record keeping audits covering 100% of specialties. • Evidence that the organisation has, through internal or independent monitoring, received assurance that procedures are being routinely applied and are achieving the desired outcomes. • Evidence that any opportunities for improvement have been captured in action plans and implementation is monitored to ensure effective completion. • Evidence of feedback to relevant professional groups (e.g. minutes, presentations).

Clinical Information Assurance - Paper Records Availability (8406)

No.	IG Requirement
8406	Procedures are in place for monitoring the availability of paper health records and tracing missing records.

Objective of the requirement

99 The organisation is assured of the availability of the health record.

100 Organisations should ensure that they are able to identify locate and retrieve information when and where it is needed. To support this, there must be effective procedures in place for monitoring and measuring paper care record availability.

Reference knowledge for auditors

101 Auditors responsible for reviewing this area and for drawing conclusions upon organisational compliance should, before they commence their review, have a thorough understanding of:

- NHS Litigation Authority: Risk Management Standards
- NHS Litigation Authority: CNST Maternity Standards
- CQC: Essential Standards of Quality and Safety
- National Archives: Records Management Standards
- DH Records Management NHS Code of Practice 2006

Table 35 Assurance required

Requirement 8406 - Paper Records Availability

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
1	There are documented and approved procedures to monitor the availability of paper care record, including tracking records and tracing missing records.	Auditors require assurance that: • The organisation has developed, approved and disseminated robust procedures based upon the latest NHS guidance.	• Policies and procedures that have been based on NHS guidance including tracking processes and tracing processes for when records are missing. • Evidence of approval of above, e.g. minutes, in accordance with organisational approval processes. • Evidence that policies and procedures have been subject to review and maintenance in accordance with review timetables (or where these do not exist, within a reasonable time period e.g. annually). • Training materials based upon approved procedures. • A training needs assessment that identifies the individuals and staff groups that require training.
2	The procedures for monitoring the availability of paper records have been implemented and action taken where availability of records is considered poor.	Auditors require assurance that: • All staff have been informed of their responsibilities and this has been supported by appropriate training; and • The strategy is available to all relevant staff and processes are in place to turn strategy into practice.	As level 1 plus: • Evidence that procedures are available to all relevant staff (e.g. via intranet). • Training records demonstrating that individuals have attended training. • Evidence that the roles and responsibilities for such individuals are included in job descriptions and objectives.

Level	Criterion	Assurance Required	Sources of Assurance/ Evidence
			- Relevant survey responses. - Discussions with staff to ascertain operational procedures and comparison of these to documented procedures (looking for differences). - Key performance indicators have been established and are monitored (e.g. for data accuracy).
3	Compliance checks are routinely undertaken to ensure staff are following the documented procedures.	Auditors require assurance that: - The organisation has in place processes to audit the application and effectiveness of its procedures; - The outcome of this audit provides assurance to the organisation that procedures are adequate and are being routinely applied.[I]	As level 2 plus: - Compliance spot check reports. - Outcomes from record keeping audits covering 100% of specialties. - Evidence that the organisation has, through internal or independent monitoring, received assurance that procedures are being routinely applied and are achieving the desired outcomes. - Evidence that any opportunities for improvement have been captured in action plans and implementation is monitored to ensure effective completion. - Documented evidence of procedural review.

[I] Note: while the IG Toolkit only requires that the organisation has monitoring and audit processes in place, auditors need to ensure that the outcomes are delivering positive assurances. Should such monitoring identify failure to apply procedures or failure to achieve objectives, this would contradict the 'picture painted' by level 2 or 3 compliance.