

An Approach to Records Management Audit

DOCUMENT CONTROL

Reference Number	Version 1.0
Amendments	
Document objectives: Guidance to help establish Records Management audits	
Date of Issue	7 May 2007

INTRODUCTION

This guidance has been developed to help organisations establish regular programmes of audit that will both demonstrate, and provide assurance of, its compliance with good practice standards laid down for Records Management,

The guidance recognises the different ways that organisations can obtain assurance of compliance and provides, as an annex, a number of checklists that can be used to measure and test compliance within the key components (the lifecycle) of records management; creation, retention, maintenance, use and disposal.

The checklists include prompts to measure good practice required across a number of standards; including: The NHS Records Management Code of Practice, the NHS Care Records Guarantee, ISO 15489 – international record keeping standards and the Information Lifecycle Management elements of the NHS Information Governance Toolkit.

What is meant by 'Audit'?

The word 'audit' is most often associated with an independent examination of financial records by external auditors or consultants, or the body or department undertaking this. In its broader context, 'audit' can be used to describe a review or scrutiny of any system, or of the processes that make up a system. The main purpose of an audit is to provide assurance that systems and processes are effective, compliant and risk free. It also provides a mechanism for regular scrutiny and improvement of systems.

What is meant by "Information Lifecycle Management?"

Information Lifecycle Management (ILM) is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence - from creation through to destruction. A records management policy will form part of an organisation's ILM, together with other processes, such as for example, a records inventory, secure storage, records audit etc. The main principles of ILM are (a) that it applies to information in paper and other physical forms, e.g. electronic, microfilm, negatives, photographs, audio or video recordings and other assets and b) that it relates to the 5 distinct phases in the life of information; creation, retention, maintenance, use and disposal.

PLANNING AND PREPARING AN AUDIT

There is no best approach to auditing compliance with records management and organisations will need to determine the most effective and appropriate approach for their particular organisation. To be effective, however, all audits, no matter how large or small, should be planned, executed and reported on in as structured a way as possible. This will ensure that:

- Responsibility for the audit is clearly defined.
- The scope and methodology of the audit is clear and the timing appropriate
- Resources required for the audit are available and at an appropriate level.
- Disruption to services is minimised
- Outcomes are identified and communicated and improvements made.

[Example of Audit Planning Document is attached at Annex 1](#)

ESTABLISHING AN AUDIT PROGRAMME

Whilst it is not essential that organisations draw up a formally documented programme of audit, such a document may help to demonstrate how, when and by whom audits are to be undertaken. A documented programme may also help organisations avoid duplication of effort and highlight gaps in the audit process.

In developing a programme it may be helpful to recognise the different sources of audit available to, and already in operation in the organisation and to consider work already agreed or scheduled for completion in the year.

[Example of an Audit Programme is provided at Annex 2.](#)

DETERMINING RESPONSIBILITY FOR AUDIT

Individual responsibility for audits will vary, depending upon the type of audit undertaken. A number of bodies external to the organisation currently undertake reviews that include assessment of some elements of records management against specific standards. These include the Healthcare Commission, The NHS Litigation Authority, the Audit Commission and other bodies supporting or governing professional practice. Records audits may also be included in the scope of an Internal or External Audit plan agreed with the Board or Audit Committee.

Where audits are undertaken at departmental level, the Departmental Manager or Director will remain responsible for overseeing the conduct of the audit and for ensuring that outcomes, including required improvements, are actioned and reported.

Irrespective of the type of audit undertaken, or the body undertaking it, it is important that the officer assigned overall organisational responsibility for records management is aware of, or appraised of, the audits beforehand. It is also important that this officer is informed of the audit outcomes and co-ordinates and reports significant findings to the Information Governance Steering Group or any supporting records management sub-group.

The Information Steering Group will be responsible for establishing a regular programme of audit for records management and for reporting updates to the Board on the progress of this, including any significant areas of non-compliance.

THE ROLE OF INTERNAL AUDIT

Internal Audit is an independent and objective appraisal service within an organisation. In the NHS it is usually provided under contract with another NHS organisation or agency, or operates as an internal function under the direct management of a nominated Executive Director.

Despite the risks, records management is often conspicuously absent from the internal audit process, possibly because records are seen in the context of other systems rather than a discrete system associated with compliance, quality and risk management. Organisations will, therefore, need to engage with both Internal and External Audit to ensure that audit resources are directed in the most efficient and effective way. Internal Audit activity is likely to focus on areas of particular risk, as highlighted in the organisation's risk register.

DECIDING THE SCOPE OF AN AUDIT

It is recommended that audits focus on those areas within the code of practice where non-compliance is most likely to constitute a risk to the organisation; this may be in terms of the organisation's legal, statutory or moral obligations or in regard to its overall reputation for maintaining high standards of records management. In this regard, organisations may wish to direct audit resources to areas where there are known problems or where these are most likely to occur.

Knowing what records are held, where they are held and who owns them is an obvious first step to deciding what and how to audit records. The existence of a records inventory, no matter how embryonic, will provide a firm basis on which to plan and execute audits that are effective and of value to the organisation; it will also help to prevent audits becoming merely expensive and time-consuming exercises of "Hunt the Record".

Separate guidance on how to carry out an Information (Records) Audit to establish a records inventory has already been developed as part of the Records Management Roadmap. This guidance is available through the following link.

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/records>

SELECTING SAMPLES

In auditing compliance with good practice in records management, evidence will need to be provided in some cases by a sample test of data and in other cases by 100% testing. The creation of records, for example should be sample tested, to provide suitable evidence to form an opinion of whether the requirement is generally satisfied. In another example, assessing whether records are stored safely and securely should usually require complete testing within a specific locality.

Sample sizes selected for testing will be dependent upon the population, i.e. the total number of records held, the resources available to do the audit and the time allowed for the audit. Clearly, the larger the sample, the more reliable the findings but there will be little value in selecting a large sample if the time allowed for the audit is consumed in locating the records rather than in examining the processes attached to them.

AUDITABLE COMPONENTS OF RECORDS MANAGEMENT

The areas designated below are those likely to require some degree of audit scrutiny, whether this is through formal, planned internal audits or departmental or operational review. Whilst Internal Audit are likely to adopt their own methodology for carrying out formal audits, it is recommended that organisations undertake regular compliance reviews to see whether they have in place, are establishing, or have still to establish good practice in regard to managing their records.

Checklists have been provided within each area to help organisations carry out these reviews. The checklists can be used, or adapted as required for both clinical and corporate records and, if appropriate, to show where improvements are needed. The completed checklists can be used to:

- Inform reports to Records Management Groups or Information Governance Steering Committees.
- Demonstrate compliance with the Records Management Code of Practice, the NHS Care Records Guarantee and Information Lifecycle Management elements of the Information Governance Toolkit.

▪ RECORDS INVENTORY

At the most basic level, a records inventory can be used to identify record series and locations which can be sampled. More sophisticated, electronic inventories may themselves facilitate in built checking of records data held, e.g. interrogation of archiving dates that have expired, identification of duplicate record sets etc.

To be effective for use in this way, it is essential that the inventory itself remains reliable. Organisations will need to regularly check the quality of their

inventory to ensure that it remains accurate enough to be used as audit source data as well as for day to day identification and retrieval of desired records.

It is recommended that audits of both the quality of the records inventory and the consistency of applying destruction review processes are carried out annually. With respect to inventory quality, the audit should verify that the inventory is accurate and that all required information is captured. As part of this evaluation, the audit should also ensure that all records scheduled for destruction are identified or “tagged” on the inventory and that destruction dates are consistent with the disposal schedules laid down in the Code of Practice.

See Annex 3. Checklist 3.1: Objective. The records inventory is accurate, up to date and reviewed annually. (See also checklist 3.4.)

- **CREATION OF RECORDS**

See Annex 3. Checklist 3.2: Objective. Records are created as relevant to the organisations clinical and corporate activities and captured into the appropriate record keeping systems upon creation or receipt

- **STORAGE OF RECORDS**

See Annex 3. Checklist 3.3: Objective. Records keeping systems and storage facilities are protected from unauthorised access, destruction or theft or from accidental damage from environmental hazards

- **ARCHIVING, DISPOSAL AND DESTRUCTION OF RECORDS**

Here, the audit should assess the actual processes involved as well as the schedules of records for archiving, disposal and destruction. The audit process needs to ensure that only those records legally eligible for destruction are being routinely destroyed in accordance with the retention schedule and that authorisation is evident.

See Annex 3. Checklist 3.4: Objective. Records are archived, destroyed or disposed of in accordance with disposal schedules

- **ELECTRONIC RECORDS**

See Annex 3. Checklist 3.5: Objective. Media and related technologies and practices for maintaining, storing and transferring electronic records are specified, designed, operated and maintained to prevent unauthorised access, corruption, damage or loss

▪ SECURITY AND CONFIDENTIALITY OF RECORDS

The NHS Care Record Guarantee sets commitments for ensuring patient information can be shared appropriately by health care staff to improve standards of care, while ensuring that it is kept securely and confidentially. The provisions of the guarantee apply to all local patient information systems, whether a new NPfIT application/compliant application or not.

Confidentiality audits may focus on controls within electronic records management systems or on paper-based systems; the primary purpose of such audits is to discover whether confidentiality has been breached, or put at risk through deliberate mis-use of systems, or as a result of weak, non-existent or poorly applied controls.

All organisations should have automated processes in place to highlight actual or potential confidentiality breaches in their patient administration systems, e.g. audit trails, failed user log-ins, antivirus, spyware etc. and to evaluate the effectiveness of controls within these systems. Ensuring regular and effective audits are in place is an essential component of the organisations board assurance and risk management process. It will also help organisations prepare for implementation of the Care Records System (CRS) which will introduce further automated control mechanisms, e.g. use of smart cards, electronic alerts and legitimate relationships (that restrict access to records to legitimate users only).

Security and confidentiality audits on paper records systems may concentrate on training, evaluation of access/ storage arrangements and review of incident reports.

[See Annex 3. Checklist 3.6: Objective. Access to records takes place in a managed manner using prescribed policies and procedures. \(See also Checklists 3.3 and 3.5.\)](#)

▪ RELIABILITY OF RECORDS

Having systems in place to ensure that records are genuine, trustworthy and legally admissible is fundamental to any records management system. Whilst focusing on systems for ensuring the accuracy and completeness of records, audits should also take into consideration the systems in place for creating, changing and retaining records to ensure that reliability is assured throughout the records lifecycle.

[See Annex 3. Checklist 3.7: Objective. Departments have taken measures locally to ensure the reliability of their records](#)

▪ RECORDS MANAGEMENT POLICY

[See Annex 3. Checklist 3.8: Objective. Records management is documented, planned and executed in a strategic and corporate manner](#)

- **RECORDS MANAGEMENT TRAINING**

[See Annex 3. Checklist 3.9: Objective. All staff receives appropriate training in records management](#)

REPORTING AUDIT OUTCOMES.

It is important that issues highlighted by audits are fed back to the appropriate managers for action. It is also important that, where appropriate, learning from the audits, including any good practice is communicated across the whole organisation and does not remain within the department carrying out the review of its records.

Significant findings from records audits, whether these are ad hoc departmental reviews, statutory audits or audits planned across the whole organisation, should be communicated to the officer assigned organisational responsibility for records management for wider dissemination. Positive outcomes should provide assurance to the Board of its records management process.

[Example of an Audit Outcomes Report and Action Plan is attached at Annex 4](#)

Annex 1: Example of Audit Planning Document

DESCRIPTION OF AUDIT	RECORDS MANAGEMENT AUDIT
OBJECTIVE.	Records are archived, destroyed or disposed of in accordance with disposal schedules (Checklist 3.4)
SCOPE:	Records held within Estates Department (May include: Buildings & Engineering records, e.g. Bills of Quantity site plans etc) Drawings, Indemnity Forms, Surveys, Inspection Reports, Title Deeds, Planning Matters, Personnel Records, Maintenance Records, Contracts and Tenders Records, Inventories, Risk and Health and Safety Records etc.
METHOD	Identify all types of records held within the department (see examples above), including electronic, paper and other media (e.g. microfiche) and select a sample of 5 record types for testing. Complete the appropriate Records Management audit checklist, ensuring where necessary that documentary evidence, including outcome of any compliance testing is appended.
SAMPLE TO BE TESTED	100% of each of the following record types: Leases Maintenance Contracts Etc.
REPORTING ARRANGEMENTS:	Director of Estates Records Manager
OFFICER UNDERTAKING AUDIT Name and Designation	A.N Other, Estates Administrative Officer
RESPONSIBLE MANAGER Name and Designation	Director of Estates
START DATE:	April 2007

Annex 2: Example of Audit Programme

Records Management Audits 2007/08					
Potential Source	Type	Scope / Area	Date	Responsible Officer(s)	Report To
Organisational/ Departmental Reviews	Example	Example.	Example	Example	Example
	<i>Clinical records audit</i>	Locality/ department based- rolling programme.	June 2007	Clinical Gov Lead	Clinical Gov. Committee
	<i>Cyclical reviews</i>	Annual review of records inventory	Sep 2007	Records Manager	Information Gov Steering Group
	<i>Compliance audits</i>	Corporate Records - Obsolete/archived records -	Aug 2007	Dept. Manager.	Records Steering Group
Internal Audit					
<i>2007/08 Audit Plan</i>	<i>Management systems</i>	Records Inventory set up and maintenance. (Phased)	2007/08	Director of Finance	Audit Committee
External Audit and Assessment					
<i>NHSLA</i>	<i>CNST/RPST</i>	Criteria relevant to records, e.g. policy	2007/08	Risk Manager	Risk / Gov Committee
<i>Healthcare Commission</i>	<i>Annual Health Check</i>	Health Check- Standards for Better Health = C9	2007/08	Chief Executive	Board
<i>Audit Commission</i>	<i>Annual plan</i>	Specific work programmes	2007/08	Chief Executive	Audit Committee/ Board

Annex 3: Checklists to measure/test compliance for key components of records management

Note. Evidence will need to be provided in some cases by a sample test of data and in other cases by 100% testing. The creation of records, for example should be sample tested, to provide suitable evidence to form an opinion of whether the requirement is generally satisfied. In another example, assessing whether records are stored safely and securely should usually require complete testing within a specific locality.

Checklist 3.1 : Records Inventory				
Objective: The records inventory is accurate, up to date and reviewed annually				
Good Practice Measure	Evidence (see note above)	Compliance Yes/No/ Partial	Action Required Yes/No	Follow-up Date
1.A Records Inventory Strategy and Procedure has been approved by the IG Steering Group				
2. A Records Inventory has been completed for the whole organisation or is underway using a stepped approach				
3. The inventory differentiates between different records types, e.g. clinical, corporate, HR, estates, financial etc				
4. The inventory differentiates between electronic and paper records				
5. The Records Inventory is reviewed annually and updated				
6. Each location on the inventory is uniquely identified.				
Compliance Testing				
<i>Review a sample of records inventory forms or other source information to check that these have been correctly and accurately entered to the inventory.</i>				

Checklist 3.2 : Creation of Records**Objective: Records are created as relevant to the organisations clinical and corporate activities and captured into the appropriate record keeping systems upon creation or receipt**

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. There is guidance on what constitutes a record and what should be done to safeguard it and make it accessible via a record keeping system within each department/ Guidance should include: Naming conventions and metadata requirements (i.e. title, subject, name of creator, date created, locality etc.)				
2. There is specific provision within the organisation's guidance for the capture, management and secure storage of electronic information (e.g. e-mails)				
3. The organisation has established a record keeping system (e.g. an electronic record management system) to manage its records	See checklist 3.5.			
4. Where a set of records is held in physical form (e.g. paper, microform) the relationships to other physical records, or to electronic records and systems, have been recorded				
5. The record keeping or record management system records the physical location of each record set				

Checklist 3.3: Storage of Records

Objective: All record keeping systems and storage facilities are protected from unauthorised access, destruction or theft or from accidental damage from environmental hazards. (See also checklist 4.5. Electronic records)

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. Storage areas allocated to hold physical records have adequate space to accommodate anticipated growth.				
2. Storage areas for physical records conform to agreed standards (e.g. BS 5454) to ensure records are safe from environmental or biological hazards, e.g. damp, fire, flood or chemical contamination.				
3. Storage areas for electronic records (including file servers) ensure records are safe from environmental or biological hazards, e.g. damp, fire, flood or chemical contamination.				
4. Electronic records are stored in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).				
5. Access to records storage areas is restricted to prevent unauthorised access, damage, theft or other catastrophic loss of records.				
6. The organisation's business continuity and/or disaster management programmes include records maintenance/management				
Compliance Testing				
<i>Review storage arrangements within a specified area/ department / locality and assess whether these comply with the good practice measures outlined above.</i>				

Checklist 3.4 : Disposal Of Records

Objective: Records are archived, destroyed or disposed of in accordance with disposal schedules

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. Procedures have been drawn up outlining methods for archiving, disposal and destruction of different record types. E.g. Confidential records are destroyed using methods which provide adequate safeguards against accidental loss, disclosure or re-construction.				
2. The organisation has a board approved records retention and disposal schedule that addresses all records created or held by the organisation. (including electronic and non-paper records)				
3. A register is maintained of all destroyed records and records pending destruction.				
4. Archiving/ disposal and destruction of records is undertaken regularly, e. g. at least annually, and with specific targets and timescales for implementation.				
5. Decisions to retain or destroy records outside of periods specified in approved retention schedules are fully documented.				
Compliance Testing				
<i>Select a sample of records held at department/ clinic/ locality level and ensure retention is in accordance with the organisations approved retention schedule.</i>				
<i>Review the register of destroyed records and ensure destruction has been undertaken in accordance with procedures and retention schedules.</i>				

Checklist 3.5: Electronic Records

Objective: Storage media and related technologies and practices for maintaining, storing and transferring electronic records are specified, designed, operated and maintained to prevent unauthorised access, corruption, damage or loss.

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
<p>1a. Documented procedures or instructions are available on the operation and use of electronic records systems :- covering:</p> <ul style="list-style-type: none"> • responsibilities; • data capture; • indexing; • authentication of records and copies; • data file transmission; • information retention; • information destruction; • backup and system recovery; • system maintenance; • security and protection; • use of contracted services; • workflow; • self-modifying files; • overlays, templates and presentation formats; • date and time stamps; • voice, audio and video data; • version control; • maintenance of documentation. <p>1b. Staff are aware of the procedures and trained appropriately</p>				
<p>2. Individuals checking data are different from those individuals inputting data. (This is particularly important where there is a risk of fraud or other malicious action).</p>				

Checklist 3.5: Electronic Records (Cont.....)				
Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
3. Procedures are in place to prevent modifications being made to stored information without detection. The electronic system must contain a secure record of all read-write accesses to the data.				
4. Levels of access available to the electronic system has been documented and approved and only permit staff with the relevant access rights to create new records or edit existing ones.				
5. There are facilities within the electronic system to ensure the integrity of data is preserved throughout. (This includes during the transfer of data to and from the storage media and protection from malicious software e.g viruses).				
6. If compound data files are used- that is files that contain other files, (for instance a word-processed document may also include a linked (but not incorporated) spreadsheet) – there are audit trails that enable the historical content of the data file to be assessed at any relevant time.				
7. Sufficient audit trail information is collected and maintained. These should: <ul style="list-style-type: none"> a. as far a possible, be generated automatically by the electronic system; b. have an accurate associated date and time; c. be available for inspection by authorised external personnel who have little or no familiarity with the electronic system; d. be kept securely to prevent any change to the data; e. not be modifiable. <p>Audit trail data is retained for as long as the data is kept.</p>				

Checklist 3.5: Electronic Records (Cont.....)				
Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
8. There are documented procedures to enable the deletion, expungement or amendment of information when it is no longer needed.				
9. IT support services have created and maintain system documentation and procedures, such as a system portfolio and change control register. The documentation provides a description of how the system operates including information about the hardware, software and network elements that comprise the electronic system and how they interact. It also records how the system is configured and any changes to the system. E.g. specification of the system, the type of network used, any software patches applied and when these were applied.				
10. Electronic records are retained in accordance with current, approved retention schedules and within appropriate environments.				
11. Storage of electronic records, particularly file servers, back up media etc is secure, appropriate and sufficient. (See checklist 3.3.)				
Compliance Testing				
<i>Obtain and review audit trail and system access reports for evidence of non-compliance with 2, 3, 4 and 6 above.</i>				
<i><u>Auditing Electronic Records</u>. An audit briefing note by the National Audit Office.</i>				

Checklist 3.6: Security and Confidentiality of Records

Objective: Access to records takes place in a managed manner using prescribed policies and procedures. (See also Checklist 3.5.)

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. Breaches of record confidentiality, loss of records etc are recorded as security incidents and managed appropriately				
2. The organisation has board approved policies for: <ul style="list-style-type: none"> o Confidentiality Code of Practice o Data Protection Act o Freedom of Information 				
3. The organisation has an appropriately supported Caldicott Guardian				
4. The organisation has developed, with other agencies. An Information Sharing Protocol to control the transfer and use of confidential records				
5. All staff are aware of their responsibilities regarding confidential records				
Compliance Testing				
<i>Obtain and review reports of any incidents relating to confidentiality breaches and ensure action has been taken to address issues. (See also tests suggested for checklists 3.3, 3.4 & 3.5.)</i>				

Checklist 3.7: Reliability of Records**Objective : Departments have taken measures locally to ensure the reliability of their records**

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. Staff validate information with patients, carers or against other records. (IGT 503)				
2. Spot checks are undertaken locally to confirm that records are an adequate reflection of what has been created or received				
3. Where evidence of non-compliance is identified guidance and training is offered				
4. Local Record Managers have been appointed				

Checklist 3.8: Records Management**Objective: Records management is organised, documented, planned and executed in a strategic and corporate manner**

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. The organisation has a Records Management Policy approved by the board.				
2. The organisation has a Board approved Records Management Strategy to deliver the policy.				
3. Records Management policies and procedures cover both clinical and corporate records				
4. Records Management policies and procedures cover both electronic and physical records				
5. Records Management policies and procedures are regularly reviewed				
Compliance Tests				
<i>Review policy content for compliance with the NHS Records Management Code of Practice.</i>				

Checklist 3.9: Records Management Training**Objective: All staff receive appropriate training in records management**

Good Practice Measure	Evidence	Compliance Yes/No/Partial	Action Required Yes/No	Follow-up Date
1. Records Management training is included in the organisation's Education, Training & Development Plan				
2. Staff understand what they are recording, how it should be recorded and why they are recording it				
3. Staff are trained to validate information with patients, carers or against other records				
4. Staff are trained to identify and correct errors				
5. Staff are advised as to the eventual use of records				
6. There is provision for the regular review of training needs in records and information management				

Annex 4: Example of an Audit Outcomes Report

Title:	Records Management Compliance Audit: Archiving, Disposal and Destruction of Records
Location / Record Type:	<i>Estates Department</i>
Date of Audit:	April 2007
Audit Undertaken By:	A.N Other, <i>Estates Administrative Officer</i>
Distribution of Report:	Director of Estates Records Manager
Objectives:	To ensure that archiving, disposal and destruction of the Trust's <i>estates</i> records is undertaken in accordance with established procedures and in compliance with the NHS Records Management Code of Practice.
Audit Scope & Methodology:	The audit was carried out using a checklist of good practice and through examination, on a test basis of records held in <i>estates</i> . These included: <i>List record types examined. E.g.</i> <i>a) Destruction register</i> <i>b) Maintenance schedules</i>
Sample Selection:	100% of records held for each type
Summary Findings:	The Estates dept has comprehensive procedures for archiving, disposal and destruction of records that comply with good practice guidelines. These, however, need to be updated to reflect retention schedules recently approved by the Board. The development of a local records inventory has commenced which, amongst other features, will allow minimum retention periods and disposal details to be entered. Destruction schedules have only been introduced in the last year and indicate that only records of a relatively minor or subsidiary nature have been destroyed in the year. The method of destruction was not recorded. A number of key records in the sample have been retained for longer than the minimum periods recommended in the NHS Records Management Code of Practice (Part 2) and in several cases, are no longer required. These are to be scheduled and approved for confidential destruction.
Appendices:	Checklist of compliance and action Supplementary working papers