Records management audit framework

Issue sheet

Document reference	NHSBSARM019
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review RM Policy\Current and Final
Title	NHSBSA Records management audit framework
Author	Rachel Hardiman
Issued to	All staff
Reason issued	Information / action
Last reviewed	24 March 2014

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Version 1	02.02.2011		IGSG	
Version 2	24.03.2014	C Dunn	RMF	Wording of roles to reflect restructure.
Version 3	31.03.2015	C Gooday	RMF	Include Public Service Pension Act 2013 in section 4
Version 3	21.03.2016	C Gooday	RMF	Links to reference documents updated
Version 4	14.10.2016	C Gooday	RMF	Links to reference documents updated

Contents

Appendices

1.   Introduction

1.1   Records management is the process by which the NHS Business Services Authority (NHSBSA) manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation to their eventual disposal.

1.2   The NHSBSA has committed itself to conducting regular audits of its records management and recordkeeping practices under Section 8 of the Records management policy (NHSBSARM001).

1.3   The Department of Health has published *An Approach to Records Management Audit* as an aid to organisations in establishing programmes of audit that will both demonstrate and provide assurance of their compliance with records management good practice standards.

1.4   Checklists derived from those included in *An Approach to Records Management Audit* are provided in an appendix to this framework document, to assist the NHSBSA in measuring the good practice required across a number of standards, including the NHS *Records Management Code of Practice* and the international recordkeeping standard ISO 15489.

1.5   This framework is designed to support and ensure the implementation of the policies and procedures governing records management in the NHSBSA, and should be read in conjunction with the following documents:

- NHSBSARM001 Records management policy
- NHSBSARM002 Records management strategy
- NHSBSARM009 Business rules for records
- NHSBSARM012 Corporate retention schedule
- NHSBSARM015 Records management guidance
- NHSBSARM017 Data storage and handling policy

1.6   Full titles, details and links to the documents cited in this section and elsewhere in this document are given in the 'References' section at the end.

2.   Scope and conduct of an audit

2.1   The audit requirement relates to all operational records held in any format by the NHSBSA, and all actions related to those records from planning and creation to ultimate disposal.

2.2   The audit should evaluate, measure and test compliance within the key components of records management: creation, retention, maintenance, use and disposal.

2.3   Audits should be planned, executed and reported on in as structured a way as possible. A model Audit Planning Document is provided in Appendix I, and a model Audit Outcomes Report in Appendix II.

2.4   Audits may be conducted across the BSA as a whole or limited to a single department or set of records, or on occasion to a single aspect of recordkeeping and records management.

2.4   The primary audit tools are the checklists provided in Appendix III. The completed checklists and audit report should be signed off by the officer or manager responsible for the audit, and presented to the HoIG / IGSG, who should oversee the implementation of any recommendations.

2.5   It is also desirable that the NHSBSA's recordkeeping is assessed from time to time for compliance with the Lord Chancellor's Code of Practice, using the self-assessment tool provided by The National Archives.

3.   Roles and responsibilities

3.1   **Chief Executive**

The Chief Executive has overall responsibility for records management in the NHSBSA. As accountable officer he is responsible for the management of the NHSBSA and for ensuring appropriate mechanisms are in place to audit the quality and compliance of the Authority's business activities.

3.2   **Head of Internal Governance (HoIG) / Information Governance and Security Group (IGSG)**

The NHSBSA's HoIG/IGSG is responsible for ensuring that this framework is implemented and kept up to date. The IGSG 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.

3.3 **Corporate Records Manager**

The officer assigned overall organisational responsibility for records management should be aware of, or apprised 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 HoIG and the IGSG.

3.4 **Local records managers**

The responsibility for local records management is devolved to the relevant Heads of Service. Where audits are undertaken at departmental level, the appropriate manager will remain responsible for overseeing the conduct of the audit and for ensuring that outcomes, including required improvements, are acted on and reported.

3.5 **All staff**

All NHSBSA staff who create, receive and use records have recordkeeping and records management responsibilities. This includes facilitating any audit of the records for which they or their business area are responsible.

4. **Legal and professional obligations**

All NHS records are Public Records under the Public Records Acts. The NHSBSA will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;
- The Pensions Act 2008;
- The Public Service Pension Act 2013
- The Occupational, Personal and Stakeholder Pension Schemes (Disclosure of Information) (Amendment) Regulations 2010;

and any new legislation affecting records management as it arises.

5. **Validity of this framework**

5.1 This framework is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

5.2 This framework should be reviewed annually under the authority of the NHSBSA Executive Board members.

Appendix A

Model audit planning document

Description of audit	Records management audit
Objective	Records are archived, destroyed or disposed of in accordance with the NHSBSA Corporate Retention Schedule (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 2011

Appendix B:
Model audit outcomes report

Title	Records Management Compliance Audit: Archiving, Disposal and Destruction of Records
Location / record type	Estates Department
Date of audit	April 2011
Audit undertaken by	A.N Other, Estates Administrative Officer
Distribution of Report	Director of Estates Records Manager
Objectives	To ensure that archiving, disposal and destruction of the Trust's Estates records is undertaken in accordance with established procedures and in compliance with the NHSBSA Records management policy and corporate retention schedule.
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 Estates. These included: [*List record types examined. e.g.*] *a) Destruction register* *b) Maintenance schedules*
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

Appendix C
Audit checklists

Checklist 1 : Records inventory (records audit)[1]				
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 IGSG				
2. A records inventory has been completed for the whole NHSBSA				
3. A records inventory has been completed for certain areas of the NHSBSA (specify)				
4. The inventory differentiates between different records types, e.g. corporate, HR, estates, financial etc.				
5. The inventory differentiates between electronic and paper records				
6. The records inventory is reviewed annually and updated				
7. Each location on the inventory is uniquely identified.				
Compliance testing				
Review a sample of records inventory forms or other source information to check that these have been correctly and accurately entered to the inventory.				

---

[1] This section should be taken to refer to the Records Audit(s) carried out in the NHSBSA. What is described as a 'records inventory' in the Connecting for Health guidance is a records-series-level audit or survey rather than a full inventory. However, the term 'records audit' is not used in this document to avoid confusion with the quite separate activity of auditing records management and recordkeeping, to which the document relates.

Checklist 2 : Creation of records

Objective: Records are created as relevant to the NHSBSA's corporate activities and captured into the appropriate recordkeeping 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 recordkeeping 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 guidance for the capture, management and secure storage of electronic information (e.g. e-mails)				
3. The NHSBSA has established a recordkeeping system (e.g. an electronic record management system) to manage its records	See checklist 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 recordkeeping or record management system records the physical location of each record set				

Checklist 3: Storage of records

Objective: All recordkeeping systems and storage facilities are protected from unauthorised access, destruction or theft and from accidental damage from environmental hazards. (See also checklist 5, Digital and 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' (BS 10008).				
5. Access to records storage areas is restricted to prevent unauthorised access, damage, theft or other loss of records.				
6. The NHSBSA's business continuity and/or disaster management programmes include records maintenance / management				
Compliance testing				
Review storage arrangements within a specified area / department / locality and assess whether these comply with the good practice measures outlined above.				

Checklist 4 : Disposal Of records

Objective: Records are archived, destroyed or disposed of in accordance with the Corporate retention schedule

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 NHSBSA has a Board-approved records retention and disposal schedule that addresses all records created or held by the organisation and that applies to all records, digital and non-digital.				
3. A register or registers is/are 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				
Select a sample of records held at department / locality level and ensure retention is in accordance with the organisations approved retention schedule.				
Review the register of destroyed records and ensure destruction has been undertaken in accordance with procedures and retention schedules.				

Checklist 5: Digital and 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
1a. Documented procedures or instructions are available on the operation and use of electronic records systems, covering: • responsibilities; • data capture; • indexing; • authentication of records and copies; • data file transmission; • information retention; • information destruction; • back-up 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. 1b. Staff are aware of the procedures and trained appropriately				
2. Inputting and checking of data is carried out by different individuals. (This is particularly important where there is a risk of fraud or other malicious action).				

Checklist 5: Digital and electronic records				
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 have been documented and approved and only staff with the relevant access rights are permitted to create new records or edit existing ones.				
5. There are facilities within the electronic system to ensure that 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. This should: 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. Audit trail data is retained for as long as the data is kept.				
8. There are documented procedures to enable the deletion, expungement or amendment of information when it is no longer needed.				

Checklist 5: Digital and electronic records				
9. IT support services have created and maintained 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*)				
Compliance testing				
Obtain and review audit trail and system access reports for evidence of non-compliance with 2, 3, 4 and 6 above.				

Checklist 6: Security and confidentiality of records

Objective: Access to records takes place in a managed manner using prescribed policies and procedures (see also Checklist 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 NHSBSA has Board-approved policies for: • Confidentiality Code of Practice • Data Protection Act • Freedom of Information				
3. The NHSBSA has an appropriately supported Caldicott Guardian				
4. The NHSBSA 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				
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, 4, and 5.)				

Checklist 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. Spot checks are undertaken locally to confirm that records are an adequate reflection of what has been created or received.				
2. Where evidence of non-compliance is identified, guidance and training is offered.				
3. Local records managers have been appointed.				

Checklist 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 NHSBSA has a Records Management Policy approved by the Board.				
2. There is 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 digital and physical records				
5. Records Management policies and procedures are regularly reviewed				
Compliance tests				
Review policy content for compliance with the NHS Records Management Code of Practice.				

Checklist 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 NHSBSA'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 identify and correct errors.				
4. Staff are advised as to the eventual use of records.				
5. There is provision for the regular review of training needs in records and information management				

Appendix D
References

Approved documents are available on the Corporate Policies and Procedures page of the NHSBSA website at http://www.nhsbsa.nhs.uk/2342.aspx

NHSBSARM001 *NHS Business Services Authority Records management policy*

NHSBSARM002 *NHS Business Services Authority Records management strategy*

NHSBSARM009 *Business rules for records*

NHSBSARM012 *Corporate records retention schedule*

NHSBSARM015 *Records management guidance*

NHSBSARM017 *Data handling and storage policy*

Department of Health and other

Department of Health *An Approach to Records Management Audit*, 2007.
http://systems.digital.nhs.uk/infogov/records/it04a.pdf

Department of Health *Records Management: NHS Code of Practice*, 2006 (Part 1), 2009 (Part 2, 2nd edn).
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

Records Management Code of Practice for Health and Social Care 2016
http://systems.digital.nhs.uk/infogov/iga/resources/rmcop/index_html

The National Archives Section 46 Self-assessment Toolkit
http://www.nationalarchives.gov.uk/documents/information-management/s46-self-assessment-toolkit-online.xls