



Health Research Authority

Document & Records Management Policy

Author: HRA Quality Assurance Manager
Date of Release: February 2009
Version No. & Status: V1 16 Final 2024 03 27
Approved By: HRA Board
Supersedes Version: V1 15 Final 2023 04 06
Review Date: March 2025
Owner: Company Secretary

1.0 BACKGROUND

1.1 Document and Record Management

Information is a corporate asset. Records are important sources of administrative, evidential and historical information. They are vital to the Health Research Authority (HRA) to support our current and future operations (including meeting the requirements of Freedom of Information and information governance legislation), for the purpose of accountability, and for an awareness and understanding of our history and procedures. This is especially true with the move towards home working, requiring an intuitive system to locate records, and the requirement for records to form a 'collective memory' for the HRA.

1.2 Definition

- A record is defined as 'recorded information, in any form, created or received and maintained by the HRA in the transaction of its business or conduct of affairs and kept as evidence of such activity'.
- Document and Records Management is an administrative system to instruct and control the creation, version control, protective marking, review, distribution, filing, retention, storage and disposal of records, that is in compliance with governance and legal requirements and undertaken in a way that meets our business needs.

2.0 PURPOSE OF POLICY

To provide advice to ensure:

- Documents and records are created, identified, protectively marked and authorised in a way that meets our business needs as well as complies with governance and legal requirements, including accessibility requirements
- Documents and records are controlled so it is clear which the current version is and which version was current at any time.
- Documents and records are available and accessible when needed.
- Documents and records are reviewed and maintained through time for as long as needed.
- Records can be interpreted and put into context e.g. who created or added to the record and when, during which business process, and how the record is related to other records.
- Records can be trusted e.g. the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- Documents and records are secure from unauthorised or inadvertent alteration or erasure and access and disclosure is properly controlled.
- Documents and records define the requirements for storage, disposal and archiving of obsolete and superseded documents.
- Records are reviewed through the appraisal process at the end of their retention period;
- Staff are trained to understand and carry out effective document control, record management and destruction.

3.0 ROLES AND RESPONSIBILITIES

- The Chief Executive has overall responsibility for records management, as the accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
- The Information Governance Steering Group (IGSG) is responsible for putting in place corporate systems and policies to ensure record capture, maintenance and disposition is part of our business.
- The Senior Information Risk Owner (SIRO) is responsible for leading and fostering a culture that values, protects, and uses information for the public good, and advises the Chief Executive on the information risk.

- The Information Asset Owners are responsible for ensuring this policy is complied with for documents and records they are responsible for.
- The Information Governance Lead has related responsibilities for ensuring documents and records across the HRA are being processed in compliance with this policy.
- All HRA employees (including temporary/contractors/secondees) are responsible for keeping full and accurate records that adequately document their business activities and complying with the Document and Records Management Policy.
- Document Authors/Owners are responsible for developing and maintaining documents using SharePoint.
- The Appraisal Committee is responsible for reviewing records (that have met the minimum retention period) to identify those;
 - of public interest worthy of permanent preservation by transfer to The National Archives or a local Place of Deposit.
 - Identify records to be retained for a longer period
 - To confirm that records not meeting above criteria should be deleted or destroyed.

4.0 SCOPE

- This policy applies to HRA produced policies, procedures, guidelines, records, including websites, social media, emails, REC/Approval documentation generated through HARP (minutes, letters, email correspondence) and instant messages.
- Key documents and records of external origin used in the regulation, development and delivery of the service are included.
- It should be noted that some aspects of the management and generation (minutes, letters, emails) of study documentation including confidentiality and archiving are covered in REC, Approval and CAG Standard Operating Procedures and managed through HARP (noting the HRA is not the primary holder of the study file and associate data – this is the Sponsor's responsibility).
- Records that are retained on outsourced systems, such as staff records on Business Shared Services (BSA), Electronic Staff Record (ESR) and finance on Shared Business Systems (SBS) are managed through ongoing contract management with retention periods specified in the Records Retention Schedule.
- Data backups, of all information technology systems, software, databases, applications and network resources needed by the HRA to conduct its business, shall be retained in line with HRA Data Retention Policy

5.0 RELATED & REFERENCE DOCUMENTS

5.1 Related HRA Documents

- Templates for HRA Policy/Procedure/instruction documents
- Over-arching policy for the management of all internal HRA policies, procedures, instructions, guidelines and forms
- HRA Staff IG Manual
- Freedom of Information policy and procedure
- Risk Management policy and procedure
- HRA accessibility guide and templates
- Records Retention Schedule
- Instruction for review of membership files and submitting to the Appraisal Committee
- Instruction for review of HARP application files over the specified retention period to the Appraisal Committee
- Instructions for transferring records to the National Archive
- ToR for the HRA Appraisal Committee
- Back up and restore policy
- Log Retention policy

5.2 Legal and Governance References

All NHS records are Public Records under the Public Records Acts. The key legal and governance references that inform the management of records are:

- The Public Records Act 1958;
- The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR);
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality and any new legislation affecting records management as it arises;
- Records Management Code of Practice for Health and Social Care 2021
- Government Website Accessibility Regulations

6.0 CONTROL OF MAJOR CORPORATE DOCUMENTS AND RECORDS

6.1 Preparation, review and approval

The decision to develop a major new policy or procedure and any associated records is the responsibility of the HRA Board, Management Groups or individual Director depending on the nature of the policy. The owner of the documents is normally the Director of the relevant HRA Division. Preparation and development may be devolved to other staff as the author, as appropriate within their area of responsibility and expertise. All internal HRA policies, procedures, instructions, guidelines and forms should be developed in line with the over-arching policy for the management of all internal HRA policies, procedures, instructions, guidelines and forms and using the approved templates (available on the SharePoint Central Library), as appropriate.

6.2 Identification, Version Control and Protective Marking

All policies/procedures and associated records should have a concise title and be produced following the HRA Policy/Procedure/instruction template available on the SharePoint Central Library. All documents should be named, version controlled and protectively marked as follows:

6.3 Naming Convention principles

6.3.1 Version Control

Documents go through a number of versions e.g.

- Working drafts
 - Final Versions
- It is important to be able to differentiate between these various drafts by giving them each their own version number and indicate within the version the reasons for changes at the back of the document making clear who is responsible for the change.
 - The version control convention used should differentiate between minor and content changes e.g.
 - Initial draft V0.1 DRAFT**
 - Changes to draft **V0.2 DRAFT**
 - Final version V1.0 FINAL**
 - Minor changes to established documents (minor being defined by approval from the Document Owner as opposed to a HRA Management Group)
 - Version V1.1 Final**
 - Content changes (content being defined by approval from a HRA Management Group as opposed to the Document Owner)
 - Version V2.0 Final**

Ensure the version number is correctly noted on the document (header/footer, front page and document control table at the back) along with detailing the changes to the document, reviewers and distribution.

6.3.2 Naming of Records

- Give a unique name to each record.
- Give a meaningful name which closely reflects the record contents.
- Express elements of the name in a structured and predictable order.
- Keep file and folder names as short as possible.
- Locate the most specific information at the beginning of the name and most general at the end.

Files/documents should be named using the following convention:

Type	Abbreviation	Type	Abbreviation
Action	Act	Plan	Pln
Agenda	Ag	Policy	Pol
Audit	Aud	Presentation	Pres
Briefing	Brf	Procedure	Proc
Form	Form	Protocol	Prot
Job description	Jobdes	Project	Proj
Memorandum	Memo	Report	Rep
Minutes	Min	Strategy	Str
Note	Not	Terms of reference	TOR

Naming files – rules:

- Keep file names short, but meaningful. Long file names mean long file paths which increase the likelihood of error, are more difficult to remember and recognise, and are more difficult to transmit in emails. However, avoid using initials, abbreviations and codes that are not commonly used.
- Avoid unnecessary repetition
- Use capital letters to delimit words, not spaces or underscores. Some software packages have difficulty recognising file names with spaces. Instead of spaces and underscores, use capitals to separate words.
- If using a number in a file name – use two digits. Unless it is a year or a number with more than two digits.
- If using a date in a file name – use YYYYMMDD. This will ensure that in a list of files in a folder, the most recent is always at the bottom.
- Using personal names. This is usually used in filing correspondence - use surname first, and then initial and the date as above. This will ensure that the correspondence will list in chronological order. This is used for complaints or committee members.
- Avoid using “draft” or “letter” at the start of names. There may be several documents in draft in a folder and it will be easier to locate the right document if it is filed by its title. Once a document has been ratified, all draft versions should be moved to a draft folder to avoid confusion as these would remain subject to the Freedom of Information Act and/or the Data Protection Act. When using Word and/or Excel, filenames and paths must always be displayed in the footer of the file.

6.3.3 Protective Marking of Documentation

The HRA will comply with the protective marking scheme established by the Cabinet Office for Government: Government Security Classifications 2014. It is the responsibility of the document owner to ensure their document is appropriately protectively marked using the guidelines, which can be found at <https://www.gov.uk/government/publications/government-security-classifications> and their awareness of its business significance and the relevant legal and governance requirements. If there is any doubt about the appropriate protection please contact the Company Secretary.

To help staff avoid handling documents inappropriately the HRA also identifies classes of documents that hold a protective status whether they are individually marked or not. These classes reflect our business needs, protect our reputation and help us comply with our legal and governance responsibilities. These classes will be reviewed by the Information Governance Steering Group (IGSG) and new classes added when necessary.

The Classes are:

- Any draft documents or records that have not been authorised.
- Any records that contain personally identifiable information.
- Any information that has been given to the HRA in confidence where the agreement to release or share has not been sought or received unless it is in the public interest to release.

6.3.4 Controlled documents

Unless stated otherwise, the electronic version of policies, procedures, instructions, guidelines and associated records held on the Central Library or the HRA website, and where appropriate on SharePoint, should be considered the controlled version. Documents should be identified and considered uncontrolled when printed unless they are managed in a controlled hard copy manual. For reference and ease of use, where possible, associated documents should be filed together with procedures, instructions and guidelines. All policies, procedures, instructions and guidelines should be issued as read only documents on the SharePoint Central Library. For those templates that require completing (e.g. the audit checklist, membership letters, etc) ensure that they are saved using a format that does not allow overwriting – for example .dot file format.

It should be noted that all documents published on the HRA Website should be published in line with the accessibility regulations – further information in regards to the acceptable format can be obtained from the Company Secretary.

7.0 RECORD CLOSURE AND RETENTION

7.1 A record should be closed when the business use for that record ceases. Following closure HRA records are subject to a minimum period of retention. The length of the retention period varies by record type and is based on legal and regulatory requirements and the assessed importance of and likely need to access the type of record. Minimum retention periods for HRA records are set out in HRA Records Retention Schedule.

7.2 The HRA Records Retention Schedule lists minimum periods of retention and in most cases, it will be appropriate to destroy records immediately once the period has expired. Before records are deleted it has to be agreed by the Appraisal Committee. Retention beyond the recommended period is permitted with good reason but if personal data is held 'longer than necessary' the HRA may breach a provision of the Data Protection Act.

7.3 Retention of Records over that stipulated in the HRA Records Retention Schedule must be agreed by the HRA Appraisal Committee.

- 7.4** Records retention is managed through the use of the records retention document libraries on SharePoint (from the 01/04/2023).

8.0 APPRAISAL

- 8.1** Lists of records due for deletion are generated through SharePoint and shared with records owners by HRA QA. Record owners are asked to confirm whether to delete, retain or transfer the records..
- 8.2** The Appraisal Committee reviews the returns and confirms the decisions on whether to delete, retain or transfer the records. Decisions are recorded using SharePoint functionality.
- 8.3** The process of selection of key corporate records for permanent preservation will be managed by the HRA Appraisal Committee who will agree to transfer to a Place of Deposit (POD) The National Archive.
- 8.4** The Appraisal Committee meets as and when required and undertakes business virtually with records of decisions recorded as per ToR. Ad hoc meetings can be arranged to review.

9.0 DISPOSAL

- 9.1** Following appraisal any records not selected for permanent preservation or a longer retention period are disposed of. No information should be destroyed if it is the subject of a request under the DPA and/or FOIA or any other legal process, such as an inquiry.
- 9.2** Paper records should be destroyed securely through a local process of cross cut shredding or using the Trust confidential waste disposal service or other similar secure disposal service.
- 9.3** Destruction of digital information is more challenging. At present there are two ways of permanently destroying digital information and these are either: overwriting the media a sufficient number of times or the physical destruction of the media. Further advice about the destruction of digital records can be obtained from the HRA Informatics service.
- 9.4** Where decisions are made to destroy/dispose of a series or bulk number of HRA records, a record of the decision and the details of the records disposed of should be maintained (through the Appraisal Committee).

10.0 E-MAIL

- 10.1** It is not necessary to keep all emails if they are not of value or importance to business as they present a significant burden on storage, creates inefficiency (time wasting searching for emails) and an increase in the risk of IG non-compliance.
- 10.2** E-mail accounts tend to be structured according to personal preference and the data stored is not searchable and organised in a systematic way, making e-mail accounts unsuitable for record storage purposes.
- 10.3** E-mail accounts should not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents. E-mails or documents distributed by e-mail that need to be retained as HRA records should be copied to the appropriate electronic file system and the e-mail copy destroyed as soon as practicable. It is important to ensure emails remain usable -emails are usable when they can:
- be opened by any user without a specific email application
 - show the full content in a readable manner to any user
 - show all attachments and allow them to be opened by any user
 - be used (forwarded, replied to etc) by any user

- 10.4** Where email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral - for example an email approving a business case must be saved with the business case file. Emails that are the sole record of an event or issue, for example an exchange between an applicant and Approval staff member should be copied to the appropriate HARP application file.
- 10.5** When a user deletes a mailbox item (such as an email message, a contact, a calendar appointment, or a task), the item is moved to the Recoverable Items folder, and into a subfolder named "Deletions". This is referred to as a soft deletion. An Exchange Online mailbox keeps deleted items for 14 days by default, but Exchange Online administrators can change this setting to increase the period up to a maximum of 30 days. Users can recover, or purge, deleted items before the retention time for a deleted item expires. To do so, they use the Recover Deleted Items feature in Microsoft Outlook or Outlook on the web.

If a user purges a deleted item by using the Recover Deleted Items feature in Outlook or Outlook on the web, this is known as a hard deletion. In Exchange Online, single item recovery is enabled by default when a new mailbox is created, so an administrator can still recover hard-deleted items before the deleted item retention period expires. Also, if a message is changed by a user or a process, copies of the original item are also retained when single item recovery is enabled.

10.6 Instant Messages

Instant messaging is used to communicate with colleagues but should not replace where a formal record is required. A screenshot should be made if a formal record of conversation is necessary and saved in the relevant folder in a usable format.

Remember that mobile messaging conversations may be subject to freedom of information (FOI) requests or subject access requests (SARs).

10.7 Approvals records

HARP is used as the repository for records relating to research ethics review and approvals including minutes, membership documents and application records. Retention of application records is managed through deletion of application documents at the end of the retention period – using flagged alert functionality.

REC Minutes are subject to transfer to the PoD as per records retention requirements and the responsibility of the annual transfer sits with HRA QA.

Destruction of membership documents - the Approval Support Member Manager is responsible for producing a MI report listing the HARP membership files due for deletion (as per records retention requirements) and submitting it the Appraisal Committee (section 8.0 above).

Destruction of application documents - the Quality and Performance Manager is responsible for producing list of application files which need to be retained (as per records retention requirements) and submitting it the Appraisal Committee (section 8.0 above).

11.0 GENERAL

Access to confidential and sensitive records should be restricted and controlled taking into account the principles contained in the NHS Code of Confidentiality.

Records related to specific procedures and activities may be identified within individual procedures and reference to HRA Records Retention periods should be included.

Records not otherwise identified including paper records, but critical to the service, are the responsibility of the individual Directors as the Information Asset Owner (IAO). The IAO should set out the requirements

for records management either within individual procedures or under separate written guidance if more appropriate. Minimum retention times must be in line with the Records Management Code of Practice for Health and Social Care 2021 and translated in the HRA Records Retention Schedule.

Records should not be routinely maintained and held on local drives (One Drive) as this can present confidentiality and access problems particularly for shared use records.

12.0 RECORDS AND DOCUMENTS OF EXTERNAL ORIGIN

Records and documents of external origin which are important for the regulation, development and delivery of the HRAs services will be held and accessed electronically document using the appropriate electronic platform (SharePoint, website, etc).

Directors, Heads of Department and Managers will ensure that any external documents are sourced, controlled and communicated as required to appropriate personnel. Where historic versions of documents are also held it will be made clear when they were in use.

For records relating to study documentation see the HRA approvals Standard Operating Procedures for guidance.

13.0 CONTROL & BACK-UP OF ELECTRONIC DATA

Electronic data will be stored and backed-up in accordance with the HRA service level agreement with Redstor. Redstor holds ISO 27001 for information Security Management, ISO 22301 for Business Continuity, and ISO 9001 for Quality Management. Redstor has also passed a Service Organisation Control 2 (SOC 2) Type 1 examination, conducted by an accredited, licensed, and independent practitioner, to verify the control and operational effectiveness an organisation has around security, availability and confidentiality.

14.0 FREEDOM OF INFORMATION

HRA, like other public bodies, complies with the requirements of the Freedom of Information Act.


15.0 DISSEMINATION AND PUBLICATION OF THE PROCEDURE

This policy, along with the policy/procedure/instruction templates, are published on the HRA SharePoint library.

Screening Questions - HRA Equality Analysis and Data Protection Impact Assessments

Equality and Data Protection Impact Assessments screening questions

For every HRA policy (defined by the Equality and Human Rights Commission as a function, strategy, procedure, practice, project or decision), please ensure the following assessments have been completed:

Assessment	Screening question	Answer	Action required
Equality	Has an Initial Equality Impact Assessment been carried out?	Yes	If no, please do so now. Do not publish the policy until the EIA is ready to be published alongside it.
Data Protection	Has a Data Protection Impact Assessment (DPIA) been carried out?	Yes	If no, please complete the  DPIA Screening template now.

Document Control

Change Record

Version Number & Status	Date of Change	Reason for Change
Version 1.1	19/4/12	Remove appendix B so that it can be made into a standalone document
Version 1.2	31/05/2012	To correct change NRES to read HRA in section 11
Version 1.3	2013 06 14	To update job titles and management groups. Release date and review date corrected to original release date.
Version 1.4	2014 05 02	To change reference from Extranet to Intranet and to update document titles.
Version 1.5	2015 03 18	Minor changes including adding reference to the Document Control System and changes to version control.
Version 1.6	2016 05 04	Annual review - update of references, roles and responsibilities
Version 1.7	2017 03 07	Information relating to management of documents on HRA Hub.
Version 1.8	2017 05 19	EIA/PIA screening questions added as per recommendation in internal audit
Version 1.9	2018 02 05	Minor revision to add clarity regarding information relating to documents and information relating to records
Version 1.10	2019 04 15	Minor changes already agreed by IGSG
Version 1.11	2019 10 09	Inclusion of reference to the HRA retention Schedule and accessibility regulations
V1.12	2020 03 11	Minor amendment - Reference to HRA Hub Guidance removed.
V1.13	2021 04 13	Minor changes including reference to Staff IG Manual.
V1.14	2022 04 12	Inclusion of Appraisal Committee along with retention, closure and disposal of records.
V1.15	2023 04 06	To include details on record naming (Based on NA advice), SharePoint records retention libraries and general update.
V1.16	2024 03 27	Minor amendments including HARP using flagged alert functionality for deletion of documents.

Reviewers

Name (name of reviewer and/or management group reviewing)	Version Reviewed
Sandra Holley, Head of QA	1.1
Sandra Holley/Jane Martin, Head of QA/Business Manager and auditor	1.2
Tom Smith, Director of Quality, Standards and Information	1.3, 1.4, V1.5
Jane Martin, HRA QA Manager	1.3, 1.4, V1.5 V1.6, V1.7, V1.8, V1.9 V1.10, V1.11, V1.12, V1.13, V1.14, V1.15, V1.16
Carla Denny, HRA QA Auditor	V1.5
Nicki Watts, HRA QA Business Support Manager	V1.5, V1.6, V1.7, V1.8 V1.10, V1.11, V1.12, V1.13, V1.14, V1.15, V1.16
Sue Bourne, Head of Guidance & Advice	V1.6
Stephen Robinson, Corporate Secretary	V1.6, V1.7, V1.9
Stephen Tebbutt, Company Secretary	V1.6, V1.7, V1.9 V1.10, V1.11, V1.13, V1.14, V1.15
IGSG	V1.10
Tim Shaw HRA IT Service Manager	V1.14, V1.15

Distribution of Approved Versions

Platform (eg HRA Atlas or Website)	Date of Publication	Version Released
HRA Website / NRES Extranet	Sent for release to website and extranet April 2012	V1.1 Final 2012 04 19
HRA Website / NRES Extranet	Sent for release to website and extranet May 2012	V1.2 Final 2012 05 31
HRA Website / NRES Extranet	Sent for release to website and extranet June 2013	V1 3 2013 06 14
HRA Intranet	Sent to release to intranet May 2014	V 1 4 final 2014 05 06
HRA Intranet	Published on Intranet March 2015	V1 5 Final 2015 03 18
HRA Intranet	04/05/16	V1.6
HRA Hub	11/04/17	V1.7
HRA Hub	22/05/2017	V1.8
HRA Hub	13/02/2018	V1.9
HRA Hub	30/04/2019	V1.10
HRA Hub	10/10/2019	V1.11
HRA Hub	11/03/2020	V1.12
HRA Hub	13/04/2021	V1.13
HRA Atlas Central Library	18/05/2022	V1.14
HRA Atlas Central Library	06/04/2023	V1.15
HRA Central Library	02/04/2024	V1.16