East London
NHS Foundation Trust

Non-Health Records Policy

Version number :	1.2
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Information Governance Steering Group
Date ratified:	March 2019
Name of originator/author:	Information Governance Manager
Executive Director lead :	Executive Director of Planning and Performance
Implementation Date :	March 2019
Last Review Date	January 2019
Next Review date:	January 2021

Services	**Applicable**
Trustwide	√
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0	14.10.11	Head of Information Governance	Final	New policy incorporating previous 'Records management procedures for non-health records', 'Records management policy'
1.1	01.03.16	Interim Head of Information Governance	Reviewed	No changes necessary
1.1	03.03.16	Interim Head of Information Governance	Final	Final version approved at IGSG
1.2	31.01.2019	Information Governance Manager	Final	Reviewed to comply with legislation.

Contents

1.0 Introduction

Records management is the process for managing records from their creation, all the way through their life cycle, to their eventual disposal, whether internally or externally generated, in any format or media type.

The Trust's records are its corporate memory. They provide evidence of actions and decisions and support daily operations. Records support policy formation and decision making, protect the interests of the Trust and support accountability, continuity, productivity and efficiency. They help deliver services in consistent and equitable ways.

2.0 Purpose

This policy sets out a framework to ensure corporate records (in all media and formats) are managed and controlled effectively, commensurate with legal, operational and information requirements.

This policy refers to corporate (non-health) records. Health records are addressed in the Health Records Policy.

3.0 Duties

Chief Executive

The Chief Executive is the Accountable Officer and has overall responsibility. The Chief Executive along with other senior managers has a duty to make arrangements for the safekeeping of records.

Senior Information Risk Officer (SIRO)

The SIRO ensures records management risks are assessed, mitigated and reported to the Board and that relevant training is provided.

Associate Director of Information Governance

The Associate Director of Information Governance is the Trust's lead for records management and is responsible for ensuring strategic, legal and operational needs are met.

Information Governance Manager

The Information Governance Manager is responsible for the day to day corporate management of records and takes a lead role in providing records management advice and support across the Trust.

Information Asset Owners (IAOs)

Service Directors are directorate Information Asset Owners with overall responsibility for the information assets within their Directorates. They will designate named individuals (Information Asset Administrators) to manage and co-ordinate records functions within their directorates.

Information Asset Administrators (IAAs)

Local records management responsibility is devolved via Service Directors to local managers and heads of department who are the Information Asset Administrators responsible for ensuring records controlled within their unit and systems are managed according to Trust policy and procedure.

All individuals

All individuals have personal responsibility for ensuring they keep accurate, timely and appropriate records that are managed in accordance with this policy and associated information governance policy. Failure to do so may result in disciplinary proceedings, litigation and dismissal.

Third parties

All third parties with access to Trust records must sign a confidentiality agreement or third party access agreement where they have direct access to trust information systems. They must assure the Trust they understand and are committed to the principles of this policy and associated information governance policies.

Information Governance Steering Group (IGSG)

The committee with responsibility for overseeing records management, monitoring compliance and effectiveness and approving records policy and strategy is the Information Governance Steering Group.

4.0 Principles

The Trust will:

- Ensure organisational arrangements are in place that support good records management
- Safely keep any records required for business, regulatory, legal and accountability purposes
- Keep its records in systems that enable records to be stored securely, with controlled access
- Maintain systems that allow records to be retrieved when necessary and disposed of when no longer required
- Maintain an inventory of its records and their location

- Ensure appropriate arrangements when its records are disclosed or held by other organisations on its behalf

This will be done through:

- A systematic and planned approach to records management from creation to disposal
- Use of filing and naming conventions
- Co-ordination of records and systems for efficiency and best value purposes
- Compliance with statutory requirements
- Awareness of the importance of records management and the need for responsibility and accountability at all levels
- Appropriate storage, retention and disposal

Its key principles are:

- Availability – records will always be available when needed
- Accessibility – the required version can be located and displayed when needed
- Interpretation – it will be possible to identify who created a record, who added to or amended it, when and how it is related to other records
- Maintenance – availability, accessibility, interpretation and trustworthiness can be maintained despite changes of format
- Security – records will be secure from unauthorised / inadvertent alteration or erasure, access and disclosure is properly controlled, the format remains readable for as long as the records are required and there is a robust audit trail
- Retention and disposal – records will be retained and disposed of appropriately according to recognised guidelines
- Training – all individuals in the Trust will be made aware of their responsibilities for record keeping
- Audit – regular audit and spot checks will take place to monitor compliance with this and associated policies, procedures and guidelines

5.0 Legal and statutory compliance

All NHS records are public records under the terms of the Public Records Act 1958 5.3 (1) – (2) and will be kept in accordance with:

- Records Management NHS Code of Practice 2006
- Freedom of Information Act 2000
- Lord Chancellor's Code of Practice issued under Section 46 of the Freedom of Information Act 2000

- Data Protection Act 2018
- Public Records Acts 1958 and 1967
- ISO17799 for Information Security and Management Systems

6.0 Definitions

6.1 Records management

Records management is the process that controls the creation, version control, distribution, filing, retention, storage and disposal of records in a way that meets the operational needs of the Trust and enables it to fulfil its legal obligations.

- Key components are:
- Record creation
- Record keeping
- Record maintenance (including tracking)
- Access and disclosure
- Closure and transfer
- Appraisal
- Archiving
- Disposal

6.2 What is a record?

A record is any recorded information, in any media or format, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of that activity.

Records are kept as evidence of the Trust's functions, decisions, processes, procedures, operations, proper conduct, rights and obligations, transactions and other activities.

Examples of records are:

- Project documentation including action plans and business cases
- Documentation about commissioned services, contracts / procurement, contractors, memorandum of understanding, SLAs etc.
- Agendas, minutes, terms of reference
- Independent / external assurance or internal audit
- Financial records, payroll, pensions information etc.
- Insurance certificates, deeds
- Job descriptions, HR files etc.

- Compliance documentation e.g. Information Governance Toolkit, NHSLA or Care Quality Commission evidence
- Training documents

This list is not exhaustive.

Draft versions are not normally records unless they have a defined value, are required for operational or legal purposes, may be required at a later date to justify decision making, demonstrate proof of process or the capability to show how an idea has evolved over time or altered in response to specific events.

Emails, records of telephone conversations, handwritten notes etc may also be records and must be retained if they have evidential weight, contribute to a decision making process or are part of the Trust's corporate memory.

Not all information is a record. Examples of documents that are NOT normally records are:

- Duplicates
- Drafts (unless they fulfil the criteria outlined above)
- Printed versions of electronic records
- Out of date distribution lists, stationary, old forms etc.
- Catalogues and trade journals
- Requests for routine information
- Non -important messages (including email) or notes that are not related to Trust business or are of a transitory nature

6.3 When does a document become a record?

A document becomes a record when it:

- Represents evidence of an activity as described above and
- Is the final non-draft version (but note that drafts may be records where there is a need for proof of process or evolvement)
- Is the original master-copy

6.4 Responsibility for ensuring information is kept as a record

Internal originators are responsible for ensuring the safekeeping of material that has records value. To prevent the retention of multiple copies, recipients are not normally responsible for saving a record unless it is received from an external originator.

Where an originator may be unaware of its relevance, the recipient has a duty to ensure it is safely kept as a record.

When there is doubt whether information is a record, the local Information Asset Administrator should decide whether it should be kept. The appropriate Information Asset Owner should be consulted where necessary. In cases of indecision, expert

guidance should be sought from the Clinical Records Development Manager or Head of Information Governance.

7.0 Records Life Cycle

Records have a life cycle. This is the life of a record from its creation / receipt to its active use, inactive retention (where it is not actively used but may be required or accessed occasionally) and finally to its disposal or archival preservation.

The stages are outlined below.

7.1 Records creation

Records should:

- Be clear, accurate and a full representation of a decision, transaction, incident or activity, show what was communicated or decided, or what action was taken
- Be created at the time of a decision, transaction, incident or activity to which they relate, or as soon as possible afterwards
- Be legible, accurate, timely and complete
- Either be explicit or have metadata (embedded information) that contains as a minimum, details of the author, dates created, modified and accessed
- Contain version control
- Named with a unique file title and meet the Trust's naming conventions
- Filed according to the Trust's filing conventions

7.2 Records storage

- Duplicate records will not be kept
- Records received or created electronically will be retained electronically. Additional copies in other formats such as paper will not be kept as a back up
- Paper records may be scanned and stored electronically provided the Trust's scanning standards for legal admissibility are met. Otherwise they should be kept in their original format
- Off-site storage may be used for records that have not been active for three years or for current infrequently used records

7.3 Records retention and disposal

- Each Directorate should undertake an annual review of its records to determine what should be retained and what can be destroyed
- All Trust records must be retained for a minimum period of time for legal, operational, research and safety reasons. Records will be kept and destroyed according to the Records Management NHS Code of Practice Records

Retention and Disposal Schedules. All destruction of records must be authorised by the Information Governance Team and subsequently Information Governance Steering Group, and clearly documented in the Trust's records inventory

- When destroying records, confidentiality must be safeguarded and the method used must secure complete illegibility (usually cross cut shredding and secure disposal of the shredded papers or incineration). Where destruction is carried out by a third party or contractor the Trust must satisfy itself all stages of destruction are secure and a Destruction Certificate obtained
- Records with long term historical or research value should be transferred to a Place of Deposit or the National Archives
- Destruction or transfer decisions must be recorded in the records inventory

8.0 Records Registration

All classes of records should be recorded at team level in a team file register. All records systems should be included in the Trust's systems inventory. The Information Governance Manager can advise further.

8.1 Vital Records

Vital records enable the Trust to continue functioning and to re-establish itself in the event of a disaster that destroys all other records. They may be held in any format.

Examples of vital records are (not exclusively):

- Legal charters, insurance certificates, deeds etc.
- Financial accounts, payroll information
- Contracts
- Intellectual property or research data
- Disaster recovery information such as out of hours contact details, estate plans

Information Asset owners should ensure preventative measures are in place:

- Identification of vital assets in the Information Asset Register supported by location of buildings, room locations and floor plans
- Identification of safe / vault combinations, passwords, cabinet / room keys etc
- Identification of vital records that are not stored correctly e.g. on desks, unlocked cabinets, not backed up
- Non -electronic information stored in a fire resistant room/ cabinet
- Backup copies of electronic information stored off site

- Plans for relocation in the event of a disaster

9.0 Filing systems

Duplicate records should not be kept. Records should therefore be filed either as paper or electronic copies.

9.1 Paper filing systems

- Use a logical file structure for paper records e.g. alphabetical or numerical
- Ensure retention schedules are factored in to make review and disposal easier
- Separate closed from open files
- Use standard cover sheets. See Appendix A for example
- Ensure file tracking and tracing is used

9.2 Electronic records systems

- Access databases must not be used as they are not supported by the Trust's ICT department
- All new systems or upgrades to existing systems must be approved for ICT, information governance and information management compliance by the Associate Director for ICT, the Head of Information Governance and the Head of Information Management respectively
- Records systems must be secure, have functionality that enables access to be restricted or locked down, include metadata and be searchable
- There must be approved and documented filing conventions for each records system

10.0 Naming and Filing Conventions

10.1 Naming conventions

Naming records consistently and logically helps distinguish similar records from each other and facilitates storage and retrieval.

- Keep file names short but meaningful
- Avoid unnecessary repetition
- Give numbers two digits e.g. 01-99 rather than 1-99 unless it is a year or number with more than two digits
- State dates 'back to front' e.g. YYYY-MM-DD (2012-01-02 for 2nd January 2012)
- Put family names first followed by initials or first names e.g. Mouse Mickey

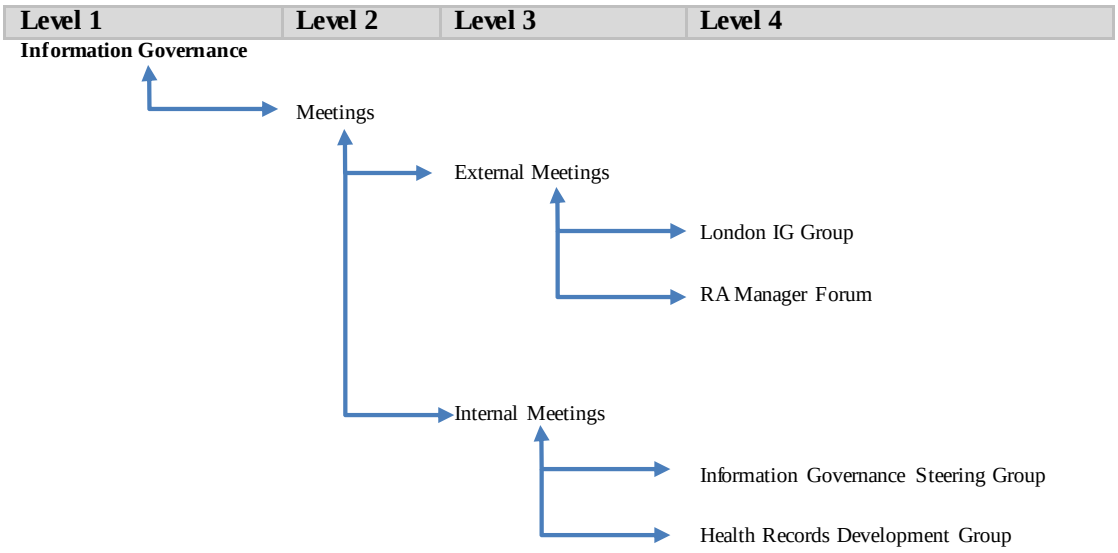
- Avoid common words e.g. ‘Draft’ or ‘Letter’ at the beginning of a file name
- Correspondence file names should include the correspondent’s name, date and whether it is incoming or outgoing
- Emails containing attachments should be saved as ‘Outlook Message Format’ type
- Versions should be indicated by the inclusion of ‘V’ followed by the Version number e.g. V1.2
- Draft versions should be indicated by the use of a number less than one followed by the word ‘Draft’ e.g. V0.1Draft
- Add the file name and path to the document footer
- Remove any hidden information e.g. track changes and comments, from the final version
- Where appropriate, add ‘Confidential and Commercially Sensitive’ to documents
- Save final documents in non-editable format such as pdf

10.2 Filing conventions

File electronic records as follows:

- Personal drive for personal documents such as supervision records, work in progress that does not currently need to be shared etc.
- Shared drive for team level information that is not confidential
- Do NOT store records on a local drive or in My Documents
- Use a hierarchical filing structure – example below.

11.0 Hierarchical File Structure Example



12.0 Scanning

Documents may be scanned and the original destroyed provided the scanned copy meets the required standards for legal admissibility. The advice and approval of the Information Governance Manager must be sought prior to commencing any scanning project.

- Do not scan documents that already exist electronically unless the scanned document adds value as a record e.g. contains a signature
- Remove all staples, clips etc prior to scanning
- Keep all pages of a document together
- Distinguish physical attachments from source documents
- Use duplex scanning including blank pages
- Ensure all documents in a batch are scanned
- Scan using a resolution of at least 200 dpi
- Artwork, line drawings, handwritten documents, photographs etc should be scanned at 300 dpi
- Where OCR techniques are applied, use 300 dpi
- Half tone material (black and white or colour separated) should be scanned at 400 dpi

13.0 Audit

Good records management needs the Trust to undertake an audit of records management systems and processes. The audit will include paper and electronic records including, but not exhaustively, those in filing cabinets, storage rooms, databases and the Trust's website.

The purpose of the audit is to ensure the Trust can:

- Enable wider internal and external audit e.g. Audit Commission, Quality Accounts, by knowing what its records assets are, and where they are located
- Protect its legal rights
- Provide authentication that its information is reliable
- Identify and take action where there is non-compliance and where improvement is necessary

The Trust will undertake regular audit to establish:

- The type of records held
- The form in which they are held
- Record keeping systems in use, their effectiveness and
- Those that need to be developed, updated or procured

As a minimum, the audit will identify where the records are stored and their:

- Condition
- Ownership
- Age
- Usage
- Historical interest

APPENDIX A. SAMPLE FILE COVER SHEET

East London NHS
NHS Foundation Trust

FILE COVER SHEET

File Reference:	
File Title:	
Volume Number:	
Filing Location:	
Department:	
Security Classification*:	
File Begins:	
File Ends:	
Disposal Due Date:	
File Transfer Date:	Moved to:
Notes:	

* Please choose from: Confidential and Commercially Sensitive Records ("Confidential"), "Internal" (shared within the Trust) or "Public" (freely available).