**Records Management Quick Reference Guide**

**Introduction**

All NHS bodies have a statutory duty to make arrangements for the safekeeping and eventual disposal of their records, including health records. This becomes more important in time of transition. All records created in the course of ICB business are public records under the terms of the Public Records Legislation.

Our records are evidence of our activities: they may be required for litigation, governance, external audits, statutory enquiries, patient care and as a basis for decision making.

Records management is the process by which an organisation manages all the aspects of records and information, from their creation through to their eventual disposal (Records Lifecycle)



**Responsibilities**

Information Asset Owners have overall responsibility for appropriate records management, including retention and disposal of information when no longer required.

**What is a record** - A record is any noted information, in any form, created or received in either paper based or electronic format and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity.

* **Corporate records (non-clinical)** - provide evidence of actions and decisions and represent a vital asset to support daily functions, operations, audit and legal requirements. Records support policy formation and managerial decision-making protect the interests of the organisation, staff, and our population. Records support consistency, continuity, efficiency and productivity and help deliver organisational priorities in consistent and equitable ways.
* **Health records (clinical) -** are also a key component of corporate documentation and are a vital asset to support delivery of safe and effective care to the ICB’s population. Although not a provider of care, the ICB will utilise health records to deliver certain duties and responsibilities (Continuing Healthcare, safeguarding, complaints, for example)
* **Email Records / Electronic Communication -** Email is a key communication tool and is not designed as an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or a formal record of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden to your organisation and information may become difficult to locate due to the size of files and attachments being stored.

NHS Mailboxes and Mailbox Archives should not be used for the long-term storage of email records.

Staff should perform regular housekeeping in their Mailboxes so that transitory and spam type emails are disposed of. Managers shall ensure all required email records are transferred from a staff leaver’s Mailbox to the approved store.

Other forms of electronic communication such as Microsoft Teams is to be used as an effective way to collaborate effectively with colleagues, conduct meetings, instant messaging but it is not designed as a long-term document storage/ management system. As with emails any recordings/documents that are records of business activity and/or formal records should be saved to the appropriate named folder on the shared network drive.

**Record Creation & Maintenance**

**Folder creation** - Each directorate/team should establish a clear folder structure that meets the organisations and directorate/department business needs that is easily understood by staff. A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records.

Staff should refrain from naming folders or files with their own name with the exception of separate secure personnel folders.

e.g.: - Corporate Governance /Annual Report/2020-21

 Corporate Governance/Annual Report/Archive/2019-20

**File Naming Convention –** A naming convention is a collection of rules which are used to specify the name of a document/record; it is best to have a unified approach. It is recommended a standard naming convention and standard terms, i.e., minutes, agendas, reports, letters received, emails received, letters sent, emails sent. Avoid non-specific or generic terms i.e., ‘General Correspondence’ or ‘Miscellaneous’. Do not name the file after the author / creator / owner

Suggested element of title

* Date
* Subject
* Document type
* Document status
* Version number
* Avoid long lengthy titles

Do not stored personal information/Business or corporate sensitive information in department/team areas. It is a legal requirement that such data is stored securely, separate secure folders should be set up with appropriate restrictions.

**Duplicate Records** - It is bad practice to duplicate information across systems. The person or team to which the record relates will normally hold the original record however occasionally duplicates may be created for legitimate business purposes. It is not necessary to keep duplicates of the same record unless it is used in another process and is then a part of a new record. Where this is not required, the original should be kept, and the duplicate destroyed. For example, documents shared for comments by numerous individuals once the final version has been approved this should remain with the team to which it relates and any duplicates to be destroyed. Meeting papers seem to be a prime culprit, there should be a centralised system for deposit available to all, with the exception of some committees such as Remuneration Committee or Part B (to be held in confidence).

**Records Inventory**- It is recommended that each directorate/team establish a log or register to aid the retrieval of folders/files. These should be reviewed annually this way you can determine if record has reached is retention period. A separate Information Asset Register is held which lists systems/information assets holding or sharing personal/business corporate sensitive information and data flows

**Disposal/Destruction**

Records should not be kept longer than is necessary and should be disposed of at the right time. Staff members must undertake regular reviews (at least annually). Review against the [Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) and schedule destruction if appropriate/required

* Two principals - destroy or to dispose
* Disposal does not necessarily mean destruction of those records – they could be transfer to another organisation/team or Place of deposit (POD)
* Destruction – records met the retention period
* Inventory of disposal/destruction should be kept.
	+ Destruction – due process followed/agreed and inventory kept by Corporate Governance Team
	+ Disposal – transferred to another organisation/team – kept by original team (IAO)
	+ Disposal – Place of Deposit – approval obtained and inventory kept by Corporate Governance Team.

**Personal Drives** - Minimise the use of personal drives, these are not to be used for ICB business as other staff may need access to the information.

**National inquiry -** particular attention should be paid to retention of records which may be required for National Inquiries eg. The COVID Inquiry. Guidance is to err on the side of caution and preserve anything that may relate to a potential public Inquiry. However, this does not remove the need for good record keeping taking place.

The expectation remains the same for good records management whether this be for a public inquiry or business as usual. It will more than likely be necessary to search for and identify relevant records, so it is essential that all records are appropriately saved and will be easily accessible.