Records Management Standards and Procedure Guidance

November 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Records Management Standards and Procedure Guidance
Date Issued:	January 2020
Date to be reviewed:	2 years after approval

Policy Title:	Records Management Standards and Procedure Guidance	
Supersedes: (Please List)	Records Management Standards and Procedure Guidance V2.2	
Description of Amendment(s):	Data Quality Housekeeping Elements	
This policy will impact on:	All Staff	
Policy Area:	Data Protection	
Version No:	3.0	
Author:	Humber IG Team	
Effective Date:	January 2020	
Review Date:	November 2021	
Equality Impact Assessment Date:	November 2019	
APPROVAL RECORD		**Date:**
	Integrated Audit and Governance Committee	January 2020
Consultation:	Information Governance Steering Group	November 2019
	Deputy Heads of Teams / Relevant Others	November 2019

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by and Date
0.1	H Sanderson	First Draft	
0.2	C Wallace	Updates and formatting corrections	
1	M Mason	Reformatted to CCG policy template	23/01/14
2	J Johnson	• Review against IGT V12 • Addition of Data Quality Requirements. • Update of Roles and Responsibilities Addition of non-compliance to the standard	TBC
2.1	C Wallace	Updated with confidentiality markers in use	
2.1	C Wallace	Reviewed with no amendments required. Reapproved for use.	8 March 2016
2.2	M Culling	Amendment to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).	16 January 2018 Integrated Audit and Governance Committee
3.0	Hayley Gillingwater	GDPR/ DPA 18 Removal of reference to eMBED Data Quality	January 2020 Integrated Audit and Governance Committee

CONTENTS

1. INTRODUCTION

Records Management is the process by which organisations manage all the aspects of records they use, whether internally or externally generated and in any format or media type, from their creation or collection, through their life cycle to their eventual disposal. The Records Management: NHS Code of Practice© was published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

The organisation's records are important sources of administrative, evidential and historical information, providing evidence of actions and decisions, and represent a vital asset to support the organisation's daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation, to support services provided and securely store personal information of staff and members of the public. Good quality records also support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

These Records Management Standards and Procedures should be read in conjunction with the NHS England Document and Records Management Policy.

2. SCOPE

This policy applies to all staff, CCG board Members, temporary staff, seconded staff, and others undertaking work on behalf of the CCG etc
These procedures relate to all records held by the CCG, in whatever format. See Annex B for examples of different types of media covered by this policy.

All records holding personal identifiable information of any individual must be managed in accordance with the Data Protection Act 2018, the General Data Protection Regulation, Human Rights Act 1998 and the Common Law Duty of Confidence.
Policy on the Data Protection and the Duty of Confidence are set out in the following organisational policy documents:
Confidentiality Policy and Confidentiality: NHS Code of Practice; and other Information Governance policies, procedures, guidance and relevant Legal and Professional obligations.

Corporate records may also be subject to the Common Law Duty of Confidence and may equally be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or disclosed. However in certain circumstances it may be appropriate to disclose certain non-personal information that has been classified as sensitive that is held by the organisation in accordance with the Freedom of Information Act 2000. For this reason it is important to implement a system of protective marking documents to indicate to the users of documents as to their level of confidentiality and how they should be treated.

All departments/business functions must identify all record management systems and ensure that appropriate records management operating instructions in accordance with these records management procedures are developed documented and made available to all staff.

All staff, including agency and temporary staff, students, volunteers and non-executive staff should be appropriately and adequately trained in the appropriate records management requirements and made aware of their responsibilities. All users of a records management system must be authorised and comply with procedures in respect of those systems, non- compliance may result in disciplinary action being taken.

See Annex C for other legal and professional obligations that must be considered.

3. POLICY PURPOSE AND AIMS

Organisational Standards

- **A register of organisational information assets is maintained** – this includes all records management systems and facilitates the maintenance of a record of Information Asset Owners and Administrators responsible for each system. ***See Information Asset Register***
- **records are available when needed** – this is to facilitate the effective continuity of day to day business, and enable a reconstruction of activities or events that have taken place;
- **records can be securely accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist. This access must be limited to staff on a need to know basis;
- **records can be interpreted** - the context of the record can be interpreted; 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** – 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;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and organisational worth can be maintained for as long as the record is needed, and on occasion permanently, despite changes of format;
- **records are secure** - from unauthorised or inadvertent alteration or erasure, and that access and disclosure are properly controlled, and ensure that audit trails will track all use and changes. Staff are confident that organisational records management procedures support them in their professional duty to protect the confidentiality of the records as appropriate. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records and documents are appropriately given a protective marking status** – this is to clearly and quickly identify the sensitivity of the document e.g. Personal Sensitive would restrict access to only a few individuals where as a Public marked document could be place on the internet website.

- **records should be protected by a contingency or business continuity plan –** protection needs to be in place for all types of records that are vital to the continued functioning of the organisation. Based on an assessment of risk and following the corporate approach documented plans should be drawn up, tested and reviewed.
- **records are retained and disposed of appropriately and securely**- using consistent, secure and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

All of the above must be documented and implemented in line with Records Management: NHS Code of Practice, and the following legislative and professional requirements:-

- Data Protection Act 2018
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Human Rights Act 1998
- The Public Records Act 1958
- The Freedom of Information Act 2000
- Access to Health Records Act 1990
- The Caldicott Report and Information Governance Review 'Caldicott 2'
- NHS Care Record Guarantee

Records Management Procedure

Registration of the Records Management System on the Corporate Information Asset Register:

It is vital that the CCG knows at all times what information assets it maintains at all times, what information those records constitute and where the information flows from and to.

The organisation will establish and maintain mechanisms through which directorates and their business functions can register all of their information assets, this includes records management systems and inventories of records. The Information Asset Register will record;

- records being maintained;
- systems used to maintain and store the records;
- associated information flows;
- the Information Asset Owner and the Information Asset Administrators for each information asset;
- information security measures put in place; and

- Business continuity plans.

This register must be reviewed regularly throughout the year by the departmental Information Asset Owner See Annex D

Data Quality

Definitions:

Data: Data is a collection of facts from which information is constructed via processing or interpretation.

Information: Information is the result of processing, gathering, manipulating and organizing data in a way that adds to the knowledge of the receiver.

Data Quality: Data quality is a measure of the degree of usefulness of data for a specific purpose.

Importance of Data Quality:

A vast amount of data is recorded when caring for patients in commissioned services. Having accurate, relevant information that is accessible at the appropriate times is essential to each and every health management or business decision and to the success of the service provided. It is therefore essential that all CCG employees recognize the importance of data quality and are aware of their responsibilities in this area.

Data Standards:

Data needs to be:

- Complete (captured in full)
- Accurate (Exact or true values)
- Relevant (meet current and potential user needs)
- Accessible (must be retrievable)
- Timely (Recorded and available as soon after an event as possible
- Valid (in an agreed format which conforms to recognized national and local standards)
- Defined (understood by all staff)
- Appropriately sought (collected or checked with a patient during a period of care)
- Appropriately recorded (in both paper and electronic formats)
- Processed in accordance with any existing data sharing agreement or data processing agreement

Data standards can be incorporated into systems either using electronic validation programmes which are conformant with NHS standards, e.g. drop down menus, or manually generated lists for services that do not yet have computer facilities. These must be controlled, maintained and updated in accordance with any changes that may occur, and in addition electronic validation programmes must not be switched off or overridden by operational staff.

Information Standards Notices (ISNs)

- The NHS communicates key changes to data standards, and deadlines affecting changes are made through ISNs. These changes must be monitored by IAOs (system administrators) to ensure that data and information systems to which ISNs apply are in compliance with the standards they specify.

- Individual systems IAOs are responsible for gaining assurance that the suppliers of the CCG information systems are updated in accordance with new ISNs to ensure systems conform to all requirements.

- From a commissioning perspective, changes need to be made to the data quality processes to ensure any changes have been implemented by suppliers of data e.g. provider services.

All CCG staff should be fully trained in record creation use and maintenance, commensurate to their roles, including having an understanding of what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:

- how to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
- why they are recording it;
- how to identify, report and correct errors;
- the use of the information and record;
- what records are used for and the importance of timeliness, accuracy and completeness;
- how to update and add information from other sources.

Synchronising information systems

In situations where data is shared or is common between systems it is imperative that the source data be validated initially. Any modifications made to this data must then be replicated in other related systems, ensuring there are no inconsistencies between them. Synchronisation between systems is required to ensure that all data sources reflect the same information.

Timescales for validation

Where inconsistencies in data and information are identified these must be acted upon in a timely fashion and documented. Locally agreed deadlines will apply to the required corrections but all amendments should be made within a maximum of two months from the identification date.
Where a data subject is making a Data Rights Request to correct or amend

inaccurate data, the process must be completed and the data subject informed within 30 calendar days under Data Protection Legislation.

External sources of data

Where possible validation processes should use accredited external sources of information, for example using Patient Demographic Service (PDS) to check NHS numbers, National Administrative Codes Set (NACS) to check organisation/GP codes, Exeter system to check deaths.

The CCG will use external sources of data to improve data quality, for example, SUS data quality dashboards on a regular basis to check comparative data and identify previously unidentified issues.

Full and accurate records must possess the following three essential characteristics:

- Content – the information it contains (text, data, symbols, numeric, images or sound);
- Structure – appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editorial devices).
- Context– background information that enhances understanding of the business environment/s to which the records relate (e.g. metadata, software) and the origin (e.g. address title, function or activity, organisation, program or department).

The structure and context of each record will alter depending on the record being created. For example, policies will need to hold contextual information like author names, review date and ratification information; whereas agenda does not require that type of information but should include attendees, venue, date and time.

Quality Checking

The CCG should establish appropriate quality checks which will minimise/eradicate errors. Consideration should be given to requiring a different member of staff to perform appropriate quality checks. Dependent on the type of record the following checks should be considered:

- ensure the correct retention period has been input onto the document which confirms the right retention/destruction period will have been calculated;
- ensure all names are spelt correctly and in the correct format;
- ensure the unique identifiers are correct and in the right format; and
- check the barcode number is correct (if relevant).

This list is not exhaustive. The Information Asset Owner is responsible for determining what types of checks may be appropriate.

It is imperative that regular validation processes and data checks/audits are undertaken on data being recorded to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include, checking for duplicate or missing data, checking for deceased patients, validating waiting lists, ensuring that national definitions and coding standards are adopted, and NHS number is used and validated.

The following validation methods may be considered:

- Bulk exception reporting; which involves a large single process of data analysis to identify all areas within a dataset where quality issues exist and to enable the correction of this data. Bulk exception reporting can sometimes be used as an initial data quality tool as this will quickly highlight any areas of concern. However, further investigation may be required to identify more specific issues.

- Regular spot checks/audits; which involves analysis of a random selection of records against source material, if available. Spot checks should be done on an ongoing regular basis to ensure the continuation of data quality. Other audits take place on an annual basis, and where an external or internal audit of a system is planned, it will include data quality.

- Data cross checking; which can also be performed on data and information held by different services and/or on separate systems. For example, secondary care data against the Exeter system to validate the recorded GP practice.

- Templates allow users to enter results and data into the patient's health record in a consistent and coherent manner. They ensure that users enter all of the required information about a patient's problem or symptom accurately and prompt the user in a logical format to enter the key information ensuring that accurate data capture occurs. The CCG assists GP practices in developing and reviewing templates to ensure consistency across the local area.

Determine the Records Management System:

This should facilitate a consistent departmental system of creating and storing records to enable information to be effectively and efficiently maintained, so that up to date and reliable records are available to staff on a need to know basis, as and when required.

Implement Secure Records Storage:

Appropriate secure storage must be implemented for the type of information held and media it is held on. The storage must offer appropriate security and protection from environmental damage, e.g. damp, fire, flood, etc. *See Annex E*

Creation and Maintenance of Records Structures:

Local records management procedures should be documented to guide staff in how to create and maintain records, including naming conventions, version control and data quality, this applies to both manual and electronic systems. These procedures should be regularly reviewed and updated where required. *See Annex F*

Creating, Accessing and Reviewing Records:

It must be ensured that access to records for any purpose whatsoever, must be strictly controlled on a need to know basis. The controls put in place will depend upon the media in which records are held and how records are stored. *See Annex G*

Protective Marking Schema:

This indicates the confidential nature of each document or record and informs staff of the appropriate level of care and confidentiality, with which the document or record should be treated. *See Annex H*

Tracking and Tracing:

It is essential that the location of records and copies of all records is known at all times*. See Annex I*

Transporting and Transferring Records:

The transportation of records and all portable media containing records are transported securely. *See Annex J*

Records Retention and Review:

The Records Management Code of Practice sets out statutory retention periods for key corporate documentation which must be followed. *See Annex K*

Secure Records Disposal:

All records must be disposed of in a secure manner to render the information illegible and non-retrievable. *See Annex L*

Incident Reporting

All incidents and near misses relating to a breach in information security must be reported using the organisation's incident reporting system.

A serious breach of security (such as a major loss of records – through fire or theft for example), must be reported and managed in accordance with the organisation's Serious Incident Policy. The organisation's Information Governance Manager must be informed as soon as possible. These incidents must also be reported to the SIRO and the CCG Management Team. These must be reported at the earliest opportunity to enable the CCG to assess the severity of the incident and escalate to the Information Commissioner's Officer within the 72 hour reporting timescale should this be required.

Any suspected thefts must be reported to the Police, by the individual responsible for the records at the time and noted on the organisation's Incident Reporting System.

It is the responsibility of the line manager, liaising with and taking advice as necessary from managers (e.g. the Information Governance Lead , , to investigate such incidents and identify any learning points that must be implemented in order to prevent a recurrence.

Disciplinary

Breaches of these procedures will be investigated and may result in the matter being treated as a disciplinary offence under the CCG disciplinary procedure. Any failure to report security breaches is likely to increase risks to individuals, our partners or the CCG and will be treated very seriously.

4. IMPACT ANALYSIS

4.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities. As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

4.2 Bribery Act 2010

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at nikki.cooper1@nhs.net.

Due consideration has been given to the Bribery Act 2010 in the development of this policy document and no specific risks were identified.

5. NHS CONSTITUTION

5.1 The CCG is committed to: Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

5.2 This Policy supports the NHS Constitution as follows:

The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

6. ROLES / RESPONSIBILITIES / DUTIES

Public Records

All NHS records are public records under the terms of the Public Records Act 1958 2.3(1)-(2). The Act sets out broad responsibilities for everyone who works with such records and provides guidance and supervision.

The NHS Code of Practice on Records Management (2006) has been developed as a guide for NHS organisations from which this policy has been produced.

Statutory Responsibility

The Secretary of State for Health, all Health Authorities and NHS trusts and other NHS bodies have a statutory duty to make arrangements for the safe-keeping and eventual disposal of their records. The Public Records Office (PRO) advises the Department of Health's Departmental Record Officer on how to manage Departmental and all types of NHS Records.

Chief Operating Officer

Overall accountability for records management across the organisation lies with the Chief Operating Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

Senior Information Risk Owner (SIRO)
The CCG SIRO is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of information are in place. The SIRO is responsible to the Governing Body for ensuring that all Information risks are recorded and mitigated where applicable. The CCG SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

Data Protection Officer (DPO)
The DPO is responsible for:

- Monitoring CCG compliance with the GDPR
- Providing advice and assistance with regards to the completion of Data Protection Impact Assessments, Data Sharing Agreements etc. Acting as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information.
- Assisting in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

Caldicott Guardian
The CCG Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Information Governance Lead
Overall responsibility for the Records Management Policy and implementation lies with the CCG Information Governance Lead Officer who has delegated responsibility for managing the development and implementation of records management procedural documents and for working with the Information Governance Team.

The CCG Information Governance Lead is responsible for co-ordinating, publicising, implementing and monitoring the records management processes and reporting issues or concerns to the Information Governance Steering Group. The Information Governance Lead is also responsible for putting systems in place to maintain the Information Asset Register. All new collections of records should be notified to the Information Governance Lead for recording in the Information Asset Register. The Information Asset Register should be regularly checked for possible errors.

Directors/Senior Managers/Information Asset Owners
Directors, Senior managers and Information Asset Owners are responsible for the quality of records management within the CCG and all line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.
All departments/business functions must identify all record management systems and ensure that appropriate records management operating instructions in

accordance with these records management procedures are developed, documented and made available to all staff.

Staff

All Staff are required to act in accordance with the principles of this policy as it relates to the management of information throughout its lifecycle. At all times staff should discharge their duties in accordance with the law, ensuring that the confidentiality and security of information is maintained and that any disclosure is appropriate and provided to an authorised recipient. In this they are supported by the Information Governance Framework, procedures and best practice guidance. This amendment was to provide better clarity on roles and responsibilities

7. IMPLEMENTATION

The policy will be disseminated by being made available on the website and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8. TRAINING AND AWARENESS

Staff will be made aware of the policy via the website.

All staff, including temps and agency staff, students and any other personnel that may be required to use systems should be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance. Misuse of the systems and the information held may be subject to investigation and disciplinary proceedings

9. MONITORING AND EFFECTIVESNESS

All departments must audit their records management systems annually, firstly to ensure that they have all been recorded on the corporate Information Asset Register and secondly to review controls within the systems and ensure that they remain appropriate and adequate to protect the information held within the system. *See Annex M.*

A checklist has been developed at Annex N to assist managers in the development of effective records management systems.

Noncompliance with this Policy by staff will be brought to the attention of the Information Governance Steering Group.

Failure to comply with the standards and appropriate governance of information as detailed in this policy and supporting procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance for which as individuals they are responsible.

Failure to maintain these standards can result in criminal proceedings against the individual

10. POLICY REVIEW

This Policy will be reviewed within 2 years from the date of implementation. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

Codes of Practice or national standards are to be introduced. These procedures will be retained in line with the Records Management: NHS Code of Practice (Department of Health, 2006) retention schedules

11. REFERENCES

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Human Rights Act 1998
- The Public Records Act 1958
- The Freedom of information Act 2000
- Access to Health Records Act 1990
- The Caldicott Report and Information Governance Revie ‘Caldicott 2’
- NHS Care Records Guarantee
- The Records Management Code of Practice

Annex A - Definitions

Term	Definition
Assembly	A collection of records. Maybe a hybrid assembly meaning where electronic and paper records are contained in one folder.
Class	Class is a subdivision or an electronic classification scheme by which the electronic file plan is organised, e.g. subject area. A class may either be sub-divided into one or more lower level classes. A class does not contain records. See folder
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Declaration	Declaration is the point at which the document (i.e. the record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Disposition	Manner in which a record is disposed of after a period of time. It is the final stage of the record management in which a record is either destroyed or permanently retained.
Document	The International Standards Organisation (ISO) standard 5127/1 states 'Recorded information shall be treated as a unit in a documentation process regardless of its physical form or characteristics'
Electronic Document	Information recorded in a manner that requires computer or other electronic device to display, interpret and process it. This includes documents (whether text, graphics or spreadsheets) generated by software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in electronic interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.
Electronic Record	An electronic record is an electronic document which has been formally declared as a corporate record. A typical electronic record consists of both electronic content (one or more

	components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.
Users(End Users)	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much or the material which constitutes the record. Since records systems tends to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.
File Plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet the records management needs.
Folder	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 (or markers where applicable). Folders are allocated into a class.
Information Asset Owner (IAO)	Is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance requirement the all Information Assets are identified and that the business importance of those assets is established.
Information Asset Administrator (IAA)	Is usually an operational manager who is familiar with information risks in their business area. Their primary role is to support the IAO to fulfil their responsibilities and ensure that policies and procedures are followed, recognise actual or potential serious incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Lifecycle Management	Information Lifecycle Management 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. Records Management policies and procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage, records audit etc.

Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record or folder.
Protective Marking	Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Record	A record in records management terminology may not be the same as a record in database terminology. A record for the purposes of this document is used to denote a 'record of activity' just as a health record is a record of activity of a patient's NHS contact. A record may be any document, email, web page, database extract or collection of these which form a record of activity. A record of activity for a database extract may therefore include a collection of health records. A formal definition is ' information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business.' (BS ISO 15489.1, Information and Documentation. Records Management)
Safe Haven	Safe Haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure person identifiable, confidential and/or sensitive information can be received, stored and communicated safely and securely. NHS England is developing an organisation safe haven procedure which will be published via the NHS England Intranet site.

Annex B - Types of Records Media

Examples of types of record and media covered by the policy include:

- Health Records (electronic or paper based).
- Emails
- Letter to and from other health professionals
- Laboratory reports
- Printouts from monitoring equipment
- Tape recordings of telephone conversations
- Administrative records (including e.g. personnel, Incident Report Forms and Risk Assessments, estates, financial and accounting records; notes associated with complaint-handling).
- X-ray and Imaging reports, photographs and other images.
- Microform (i.e. fiche/film).
- Audio and videotapes, cassettes, CD-ROM etc.
- Computer databases, output, and disks etc., and all other electronic records.
- Material intended for short term or transitory use, including notes and ‘spare copies’ of documents.

This list is not exhaustive.

Annex C - Legal and Professional Requirements

- Records Management: NHS Code of Practice
- Data Protection Act 2018
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Human Rights Act 1998
- The Public Records Act 1958
- The Freedom of Information Act 2000
- Access to Health Records Act 1990
- The Caldicott Report
- The Information Governance Review; ‘Caldicott 2’
- Information: ‘To share or not to share’, (the government response to Caldicott 2)
- HSCIC: A Guide to Confidentiality in Health and Social Care
- NHS Care Record Guarantee
- NHS England Policies

Annex D - Registration of Records Management Systems.

1. The types of records that should be recorded on the corporate information asset register:

- Personnel records
- Financial papers
- Estates papers
- Service Provision records
- Performance monitoring
- Policy papers (reports, correspondence, etc)
- Minutes, circulated papers etc of meetings
- Complaints papers and correspondence
- Research and development papers

This list is not exhaustive.

Clinical care records are not specifically covered by these procedures. However where clinical or care records are being maintained records management procedures should be developed in line with professional standards and the Records Management NHS Code of Practice. These must also be registered on the corporate information asset register.

Where a record collection identified or created contains personal confidential information, an information flow must be completed and returned to the Information Governance Team. This enables the organisation to assess how it uses personal confidential information, ensure that this is undertaken on a legal basis and ensure appropriate controls are put in place to securely protect the confidentiality of that information.

Registration of an information asset will be achieved by the allocation of a unique identifier.

Registration systems should be monitored regularly and reviewed throughout the year at the same time as the register is reviewed to ensure that systems continue to operate effectively and efficiently and meet the needs of users.

All records held by the organisation that are listed within the Retention and Disposal Schedule of the Records Management: NHS Code of Practice and any organisational additions require registration.

Annex E - Secure Storage of Records

Appropriate secure storage must be implemented in respect of the type of records being held and the method in which they are held.

Manual Records

Sufficient security should be implemented to protect confidentiality of both person identifiable and personal confidential information, and corporately and commercially sensitive information. This may be implemented in a number of ways, but must be suitable for the sensitivity of the records and the method in which it is stored. The following should all be considered;

- Restricting access to the building or parts of the building;
- Restricting access to offices on a need basis;
- Use of lockable filing cabinets;
- Desks with lockable drawers;
- Specifically designed secure storage cupboards; and
- Specialist storage boxes for different types of storage media e.g. microfiche or photographic images.

This list is not exhaustive, dependent on the records being maintained more specialist storage methods may be required.

Consideration must also be given to the prevention of damage or deterioration due to such environmental situations such as damp, excessive heat or light, flood or fire.

Bulk Storage – Current Records

Storage facilities for current records in use must be secure and located in a manner that enables speedy access by authorised users. This may be:

- In approved central or local filing systems e.g. for common corporate files or patient record files.

All records must be kept securely at all times and when a room containing records is left unattended it must be locked.

An appropriate sensible balance should be achieved between the needs for security and accessibility.

Decisions on the suitability of office filing equipment must take the following factors into account:

- Compliance with Health & Safety regulations.
- Users' needs, usage and frequency of retrievals.
- Security (especially for confidential material).
- Type(s) of records to be stored and their size and quantities.
- Suitability, space efficiency and price.
- Fire-proofing and water-proofing.
- Protection from environmental damage (e.g. light damage to negatives).

Appropriate advice on the above will be provided Information Governance Team or the Health and Safety Representative.

Bulk Storage - Semi-Current Records

Semi-current records contain information that is required on an infrequent basis.

As the need for quick access to particular records reduces, it may be more efficient to move the less frequently used material out of the immediate work area and into a secure archive store.

An appropriate sensible balance should be achieved between the needs for security and accessibility.

Such records should:

- Not need to be retrieved quickly or frequently.
- Be accessible.
- Be stored in a format and state that complies with the Information Security Policy.
- Be stored in a secure records store that:
    - Is kept locked at all times
    - Has access restricted to relevant staff only
    - Is fitted with a suitable fire door
    - Is fitted with a suitable smoke/fire detector
    - Is fitted with window bars where the store is on the ground floor and has windows next to public areas
    - Is safe from any form of environmental damage to the records (e.g. damp etc)

- Be compliant with the Record Retention Periods set out in Department of Health guidance 'Records Management: NHS Code of Practice'.
- Be stored in a manner that conforms to Health and Safety Policy.
- Be stored in a manner to prevent deterioration or loss.

Non-Current Records

Storage of non-current records should be in accordance with the requirements set out in section on semi-current records.

The Department of Health guidance 'Records Management: NHS Code of Practice' takes account of the legal requirements and sets the minimum retention periods for both clinical and non-clinical records and must be followed.

The organisation has local discretion to keep material for longer, subject to local needs, cost, and, where records contain personal information, in line the requirements of the Data Protection Act 2018 and of the General Data Protection Regulation.

Off-Site Storage

Records should only ever be taken off site with the appropriate approval and in accordance with the Safe Haven Policy and guidance. These require staff to give the highest priority to the security of these records held off site, especially in the case of confidential records.

A records tracking system must be implemented to record the location of files at all times, this includes photocopies of manual files and printed copies of electronic files. Staff must be trained in the completion of the tracking system and must complete it for all files taken off site.

The Information Governance Team can provide further advice.

Where a number of records need be carried during the day and they cannot practicably and securely remain with the member of staff transporting them then they must be locked out of sight in the boot of the car, during appointments. **NB/** This method of storage is only to be used for the short term, records must never be left in the boot of the car for long periods of time or overnight. All records removed from the boot of the car must be carried in a secure container e.g. lockable brief case.

If records are to be taken home, the records must be stored securely in accordance with the staff members' Professional Code of Conduct and this policy in conjunction with the Safe Haven Policy and guidance. It is essential that any such records are logged out of the department, using the implemented tracking system to ensure that records removed are trackable at all times.

Where records need to be taken home, for example where they are needed for or an early appointment the next day, they must be stored in a manner so that others members of the household or visitors can not view them and they should be placed somewhere secure within the home.

Records should not be left in vehicles unless it is absolutely necessary. In such circumstances they must be left out of sight, ideally in the boot, and the vehicle must be locked.

Electronic Records

As with manual records electronic records must be appropriately protected from unauthorised access and deliberate or accidental loss or destruction. The following should be considered

- Use of secure corporate network folders
- Appropriate password controls, including access levels,
- Encryption of equipment used,
- Use of Kingston Locks to secure portable electronic equipment,
- Appropriate physical security to prevent access to the electronic equipment. These are likely to be the same as above.
- Appropriate backup and recovery procedures

This list is not exhaustive

Using the approved corporate network storage all files should be stored in line with requirements of the corporate records management structure to enable security and ease of:

- Storage and back-up.
- Access control, based on the need to know Caldicott Principle, this must be documented and kept up to date.

The preferred method of access to electronic information is from the secure network, the organisation will provide authorised encrypted mechanisms to achieve this whilst off site, where required and authorised. However on the few occasions where it is not possible to access information in this way, any information held outside of the secure network must be held only on authorised, encrypted equipment that has been issued by the organisation.

All information must always be returned to the secure network, as soon as possible, to ensure the most up to date information is held on the secure network. When copies of the information have been successfully returned to the secure network, any copies held away for the secure network must be securely removed from the portable equipment. (Separate approved contractual arrangements will be made for information processed by third parties)

Where a number of records need be carried, in electronic format on approved equipment, during the day and they cannot practicably and securely remain with the member of staff carrying them then they must be locked out of site in the boot of the car, e.g. during appointments. This method of storage of equipment is only to be used for the short term. Records and equipment must never be left in the boot of the car for long periods of time or overnight. All records and equipment removed from the boot of the car must be carried in a suitable container.

Where records need to be taken home on approved equipment, for example where they are needed for or an early appointment the next day, the equipment must be stored in a manner so that others members of the household or visitors can not view these records, i.e. in a suitable container and placed somewhere secure within in the home.

Other Media

Microfilm and Fiche (Microform)

Microform can be in roll film format or in microfiche format. Master negative and working positive copies should be made. Only the positive copies should be used for reference purposes.

Master copies should be stored in closed non-airtight containers made of non-corrosive materials, such as inert plastic. Containers should also be free of bleaching agents, glues and varnishes. These should be held securely and checked regularly for deterioration.

Rolls of film should be mounted on inert reels and secured by the use of acid free paper ties. Fiche and jacketed film should be stored in acid-free envelopes.

Rubber bands and paper clips should not be used.

Microform should be stored in controlled atmospheric conditions, with temperature between 15 and 20 degrees centigrade (ideally not exceeding 18 degrees).

All storage areas must have appropriate physical security in place.

Visual Images

In the case of photographs, video or DVD recordings, the quality of the images available from negatives or original prints/recordings should be considered and new prints/recordings may be made in cases where the original is deteriorating.

Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Sound recordings and video recordings (tape and DVDs) should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

All storage areas must have appropriate physical security in place.

In every case visual and audio recordings will only be made after proper informed consent has been obtained, from patients, staff and/or visitors. This includes situations where the police wish to take a photograph to assist their enquiries, unless there is a mental capacity issue.

All photos or video gathered should be done so on equipment that it owned by the organisation with due care and attention paid to its storage.

Scanning

The option of scanning paper records into electronic format may be considered for reasons of business efficiency, to address problems with storage space or to include a record of a paper document within an existing electronic record.

Where this is proposed, the following factors should be taken into account:

- Costs.
- Archival Value.
- The need to protect the evidential value of the record by copying and storing the document electronically.
- In accordance with British Standards. In particular, the Code of Practice of Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP 0008) should be adhered to.
- Current regulations relating to the use of scanned documents with existing electronic records.

Annex F - Creation and Maintenance of Records Structures

Paper Records

A clear and logical filing structure that aids retrieval of records should be used; ideally this structure should follow a corporate system of filing paper records to ensure consistency. However if this is not possible then the system of allocating names to files and folders should allow intuitive filing.

Individual Record Folders

A referencing system should be implemented which meets the organisation's and directorate's business needs, and can be easily understood by all members of staff that create documents and records. The referencing can be, alphabetic, numeric or alphanumeric.

Individual record folders should be indexed and enable ease of adding information to different sections, they must be designed in line with any local practices which are based on professional guidance for which the records are used.

Where duplicate carbonised forms are used, the original top copy should be retained by the organisation due to the eventual deterioration in quality of archived carbonised paper records. Each copy must state who that copy belongs to and where it should be sent.

All storage areas must have appropriate physical security in place.

Referencing: Each Directorate should establish and ensure compliance to a document referencing system that meets its business needs and is easily understood by staff members that create, file or retrieve records held in any media. Several types of referencing can be used, e.g. alpha-numeric, alphabetic, numeric or keyword. The most common of these is alpha-numeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the records are kept, and identify the record by reference to date and format.

Naming: Each Directorate should nominate staff to establish and document file naming conventions in line with national archives advice; i.e.

- Give a unique name to each record,
- Give a meaningful name which closely reflects the records contents,
- Express elements of the name in a structured and predictable order,
- Locate the most specific information at the beginning of the name and the most general at the end,

- Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

Indexing and Filing: Each Directorate should establish and document a clear and logical filing structure that aids retrieval of records. The register or index is a signpost to where paper corporate records are stored, e.g. the relevant folder or file, however it can be used as a guide to the information contained in those records. The register should be arranged in a user friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear logical names that follow the organisation's or directorate's naming convention

The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. Filing of corporate records to local drives on PC's and laptops is not appropriate, files must be saved to the departmental network, to ensure only authorised access is available and that appropriate backups are taken. Likewise, the filing of key organisational paper records or clinical records in desk drawers is not appropriate, departmental accessible secure storage should be used.

Version Control: A system of version control must be implemented to enable staff to know that they are working the latest/correct version of the documentation. This may be in form of a version number and date or by use of document creation date.

Annex G - Creating, Accessing and Reviewing Records

When records are created and/or updated, it is essential that indices are first checked to avoid the creation of duplicate records. This will ensure that all information and records in relation to the same project are maintained in one place.

Local procedures should be put into place to ensure robust records management and data quality processes as appropriate for the system. This applies to both manual and electronic systems. These procedures should be regularly reviewed to ensure that they remain appropriate to the records to be maintained and updated where required.

All Records

All record entries must:

- Contain a filing index and section dividers (manual records)
- Named in line with the local naming conventions.
- Be factual, consistent, accurate and consecutive.
- Be recorded as soon as possible after an event has occurred.
- Be accurately dated, timed and signed, where required.
- Use of abbreviations should be kept to a minimum. If abbreviations are used, they should be from an agreed list which is formally maintained and can be made available on request.
- Provide clear evidence of action taken or to be taken.
- Record risks or problems identified and action taken to deal with them.
- Errors should have a single line used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment
- Be bound and stored so that loss of documents is minimized.
- Have an integral audit trail.
- Records should be readable when photocopied or scanned
- Do not alter or destroy any records without being authorised to do so
- NEVER falsify records

Personal Data

Under the requirements of DPA – Part II, subject to specific provisions referred to below, an individual is entitled to be:

- Informed whether their personal data are being processed by the organisation.
- Advised of the nature of the data, the purposes for such being processed and with whom it is being disclosed.
- Informed of the data held and its source(s).

- And have access to information held about them, subject to certain exemptions. Please see the Subject Access Policy for further guidance.

Annex H - Protective Marking Schema

This scheme is as per the NHS England Document and Records Management Policy.

Classification of NHS Information – Marking Guidance

NHS CONFIDENTIAL – appropriate to paper and electronic documents and files containing person-identifiable information, including service users, staff and any other sensitive information. Where the document is considered very confidential then this should be printed on pink paper so it is clear that the document is to be treated appropriately.

NHS PROTECT - Discretionary marking that may be used for information classified below NHS Confidential but requiring care in handling. Descriptors may also be used as required.

Table of descriptors that may be used with 'NHS CONFIDENTIAL' or 'NHS PROTECT' marking	
Category	**Definition**
Appointments	Concerning actual or potential appointments not yet announced
Barred	Where: - -there is a statutory(Act of Parliament or European Law) prohibition on disclosure, or -disclosure would constitute a contempt of court (information the subject of a court order)
Board	Documents for consideration by an organisation's Board of Directors, initially in private. (Note: This category is not appropriate to a document that could be categorised in some other way)
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
Contracts	Concerning tenders under consideration and the terms of tenders accepted.
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
Management	Concerning policy and planning affecting the interests of groups of staff. (Note: Likely to be exempt only in respect of some health and safety issues.)
Patient Information	Concerning identifiable information about patients.

Personal	Concerning matters personal to the sender and/or recipient.
Policy	Issues of approach or direction on which the organization needs to take a decision (often information that will later be published)
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.
Staff	Concerning identifiable information about staff.

Annex I - Tracking and Tracing Mechanisms

The accurate recording and knowledge of the whereabouts of all records, including copies, regardless of the media they are held on is essential to the maintenance of confidentiality, and should also provide a mechanism to ensure appropriate security of records is in place at all times.

Formal procedures for tracking and tracing of records should be implemented to enable the directorates and business functions of the organisation to continue without unnecessary disruption and facilitate the identification of the location of records at all times.

Tracking Mechanisms for all records regardless of the media

Directorates must ensure that all departments have tracking and tracing systems in place to record the movement and location of records and provide an auditable trail. The following information should be recorded as a minimum:

- The reason for the removal or transfer of the record or copy of record, including appropriate authorisation and details of who it is to be shared with
- The name of the record
- The media it is held on
- The method of transfer
- The person who has removed the record
- The person, unit, department or place to which it is being sent or taken
- The date of removal or transfer of the record
- Signature of the person removing it
- The expected and actual date of return of the records or if it is a permanent transfer.
- Signature and date of the person returning it.

Each tracking system, manual or electronic, must meet all user needs and be supported by adequate equipment and should provide an up-to-date and easily accessible movement history and audit trail.

Since the success of any tracking system depends on the people using it, all staff must be made aware of its importance and given adequate training and updating.

Tracking systems must be capable of recording where records are passed between members of staff whilst away from their secure storage point.

Tracking systems must be implemented and reviewed annually or after any serious untoward incident for operational effectiveness.

Manually operated tracking systems

All files/ records must be recorded within the tracking system to facilitate traceability when removed from the department/ building that stores them.

Acceptable methods for manually tracking the movements of active records include the use of:

- A paper register – a book, diary, or index card to record transfers
- File “on loan” (library-type) cards for each absent file, held in alphabetical or numeric order
- File “absence” or “tracer” cards put in place of absent files

Where manual tracking systems are used they must be kept up to date otherwise the system will quickly be rendered ineffective.

Electronically operated tracking systems

Acceptable methods of tracking include the use of:

- A computer database with clearly defined access permission rights.
- Bar code labels and readers linked to computers.
- Workflow software to electronically track documents.
- Functionality built into any electronic records management systems.

Electronic tracking systems are a preferred option; if used, the Records

Manager should be contacted and will advise of the appropriate procedure to be followed.

Where electronic tracking systems are used, staff must be fully trained; otherwise the system will quickly be rendered ineffective.

Annex J - Transporting Records

This section covers transport between:

- Organisation's sites
- Organisation's sites and other NHS or Non-NHS sites.

Transporting Records

Any transportation of records, including copies, in whatever media must always have the appropriate authorisation, and must be recorded in the relevant departmental tracking system.

Mailing of Paper Records by Post or Courier

There are various options available if records are to be mailed. The Government has provided minimum security measures for such eventualities which the organisation was required to adopt.

Transporting by hand

When staff are transporting information off site they must obtain the appropriate authorisation and ensure that they are carried in an appropriately secure manner, which includes the requirement to transport sensitive personal information in a suitable container or folder, and in an encrypted format where held electronically. These measures will help provide appropriate protection from damage, unauthorised access, such as theft or loss.

Handling Records

The following rules must be applied when handling records

- No one should eat, drink or smoke near the records.
- Records containing personal confidential information being carried on-site, e.g. from the archive storage to the department, etc. should never be left unsupervised and should be enclosed in a container e.g. an sealed case or covered trolley, to prevent unauthorised access whilst in transit.
- Records should be handled carefully when being loaded, transported or unloaded. Records should never be thrown.
- Records should be packed carefully into vehicles to ensure that they will not be damaged by the movement of the vehicle.
- Records transported in vehicles must be fully enclosed so that they are protected from exposure to the weather, excessive light and other risks such as theft.

- No other materials that could cause risks to records (such as liquids or chemicals) should be transported with records.

- Where records or equipment holding records need to be left in a vehicle for a short period of time it must be ensured that they are locked out of sight in the boot of the car. This method of storage is only to be used for the short term. Records must never be left in the boot of the car for long periods of time or overnight. All records removed from the boot of the car must be carried in a container.

Emailing Records

Transport of electronic documents, including via e-mail must be undertaken in a secure manner.

Records containing person identifiable or personal confidential information must only be emailed via NHS Mail. i.e. both to and from an NHS Mail account as this provides appropriate encryption.

Where there is a requirement to email person identifiable or personal confidential information to non-NHS Mail accounts (for example a local authority .gov.uk email account) this must be done only after consultation with the Information Governance Lead and completion of any necessary security checks or Data Protection Impact Assessments.

Where records are received by email they must be added to the appropriate record as soon as possible to ensure completeness, once the information is added to the record the email should be deleted.

Annex K - Records Retention and Review

General Principles

Records should be kept only for as long as they are required subject an appraisal process to determine whether they are still in use or are of permanent archival value.

When various versions of documents are produced prior to agreement of a final version, unless there is a reason to keep these, they should no longer be retained.

Preceding documents should be retained if the undated version contains significant major changes to content, as this will form the version history of the document.

Where different versions are to be retained a version control mechanism must be implemented.

Records containing personal information should only be retained as long as the purpose for holding the information applies.

The organisation has adopted the retention periods for health and non-health records as set out in the Records Management: NHS Code of Practice (Department of Health, January 2009) as detailed in Part Two of the Code available from the Information Governance pages (IG Policies & Guidelines) of the organisation's staff website. The retention schedule will be reviewed annually by the Records Manager, and maintained in accordance with the NHS Records Management Code of Practice. Evidence of this process and communication of relevant up dates will be reported to the Information Governance Steering Group.

The retention of records for longer than the recommended period must be discussed with the organisation's Information Governance Manager and, with their agreement, may be justified in writing for ratification by the Caldicott Guardian and/or SIRO.

Service Managers and Line Manager as responsible for ensuring that there is a documented records management process in place within their area. This should document how records are managed, indexed and how destruction dates are managed.

Destruction dates could be managed in a number of ways:-

- Destructions dates noted within headers/footers;
- Dates tagged onto the end of file names;
- Dedicated electronic filing systems can be used that ask for a destruction date when a file is uploaded; and
- Destructions dates listed within filing index with annual review to action.

This list is not exhaustive.

Annex L - Secure Disposal of Records

When it has been determined that record(s) have reached the retention period then it must be recorded in a register of disposal and appropriate management authorisation for destruction obtained.

The method used to destroy all records must be fully effective and secure their complete illegibility, e.g. an approved shredding service.

Except for early versions of completed documents, a brief description must be kept in the organisation's disposal register of everything that has been destroyed, identifying:

- The document
- When destroyed and by whom.

The Information Governance Team should be consulted for advice and guidance.

Disposal of Documents

Following appropriate appraisal of the records to identify any records that should be retained, paper records or documents may be disposed of via shredding, pulping, or incineration this process should be undertaken at least annually. This can be done on site, or via an approved contractor who will provide certificates of destruction.

All approved Contractors must have a current contract in place containing all relevant Information Governance clauses, refer to the Information Governance Leadfor details.

Disposal of Records held in Electronic Format

Following appropriate appraisal of the records to identify any records that should be retained, the disposal of documents held in electronic format must be completed by a method which ensures that the information cannot be retrieved from the electronic media on which it was held. This can be done on site, or via an approved contractor.

Destruction of files and/or electronic media must be undertaken by the IT Department to ensure that all records to be destroyed are done securely.

Register of Destruction of Records

Description of Records identified for Destruction & Dates covered and volume.	**Retention Period checked against Records Management CoP. Y/N**	**Destruction authorised by.**	**Date and Method of Destruction**	**Certificate of obstruction obtained and filed.**

Annex M - Audit of Records Management Systems

The organisation will regularly audit its records management practices for compliance with this framework.

Audits will:

- Identify all records management systems in use and ensure they are recorded on the organisation's Information Asset Register.
- Identify areas of operation that are covered by the organisation's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

There are two types of records audit that must be carried out on an annual basis:

Records Management Audit

As part of the Information Governance Assurance Programme and to meet the requirements of the Freedom of Information Act 2000, all NHS organisations are required to regularly audit their Records Management Practices. This is to be carried out at all locations on an annual basis by the Local Records Managers. The Local Records Manager is to use the Records Management Audit tool detailed in Annex F. The completed audit is to be submitted to The Records Manager, who may, supported by the Information Governance Team, if deemed necessary conduct a more detailed audit at any location. Further information regarding this audit is available from the Records Manager.

Information Flows Mapping and Audit

As part of the Information Governance Assurance Programme, all NHS organisations are required to have an up-to-date register of the information they hold and understand how it is handled and transferred to others. The mapping of routine information flows, using the data mapping tool available on the information governance pages on the intranet, will help the organisation identify how and when person identifiable information is transferred into and out of the organisation and form part of the required register. More importantly it will allow the organisation to assess and address risks to ensure that sensitive and or personal information is transferred with

appropriate regard to its security and confidentiality, and ensure that staff are provided with clear local procedures that meet organisational and national standards regarding the handling of personal information. Risks identified as part of this process must be added to the appropriate risk register. Directorates must nominate appropriate staff to complete and report on the mapping of information flows. The Information Governance Team will support this work by providing information mapping tools, safe haven material, organisational policies, procedures, guidance, and additional auditing as appropriate. All information mapping reports must be provided to the Information Governance Team within a time frame specified in the audit schedule. An audit schedule will be approved by IGSG and issued by the Information Governance Team any significant risks arising from the results of reports or audits will be recorded on the departmental risk register and reported to the IGSG which is chaired by the SIRO.

Annex N - Records Management Checklist

No.	System Requirement	Description	Guidance Reference	Complete Y/N
1.	**Registration of the Records Management System on the Corporate Information Asset Register**	All records management systems in place, including databases and spreadsheets should be registered on the organisation Information Asset Register. The Information Asset Owners and Administrators should be identified and recorded for each information asset registered.	Annex D and the Information Asset Register	
2.	**Determine the Records Management System**	Clear determination of aims and requirements, and information flows will assist in effective design of consistent recording and secure storage and use of information.		
3.	**Implement secure records storage**	Appropriate secure storage must be implemented for the type of information held and media it is held on	Annex E	
4.	**Creation and Maintenance of Records Structures**	Local records management procedures should be documented to	Annex F	

		guide staff in how to create and maintain records, including naming conventions, version control and data quality, this applies to both manual and electronic systems		
5.	**Creating, Accessing and Reviewing Records**	It must be ensured that access to records for any purpose whatsoever, must be strictly controlled no a need to know basis. The controls put in place will depend upon the media in which records are held and how records are stored.	Annex G	
6.	**Protective Marking Schema**.	This indicates of the confidential nature of each document or record and informs staff of the appropriate level of care and confidentiality with which the document or record should be treated.	Annex H	
7.	**Tracking and Tracing**	This facilitates a mechanism by which the location of records or copies of records can be known at all times**.**	Annex I	
8.	**Transporting and**	The transportation of records,	Annex J	

	Transferring Records	documents and all portable media containing records must be transported securely.		
9.	**Records Retention and Review**	The Records Management Code of Practice sets out statutory retention periods for key corporate documentation which must be followed.	Annex K	
10.	**Secure Records Disposal**	All records must be disposed of in a secure manner to render the information illegible and non-retrievable.	Annex L	
11.	**Audit of Records Management Systems**	All departments must audit their records management systems annually firstly to ensure that they have all been recorded on the corporate Information Asset Register and secondly to review controls within the systems and ensure that they remain appropriate and adequate to protect the information held within the system.	Annex M.	

APPENDIX 1

Creating a healthier Hull

NHS Hull Clinical Commissioning Group

Please refer to the EIA Overview & Navigation Guidelines located in *Y:\HULLCCG\Corporate Templates and Forms\Equality and Diversity Information* before completing your EIA)

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Records Management Standards and Procedure Guidance
Date of Analysis:	12/11/2019
Completed by: **(Name and Department)**	Hayley Gillingwater Senior Information Governance Specialist
What are the aims and intended effects of this policy, project or function?	The overall purpose of the policy is to set out the CCG's approach to the Management of Health Records within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation to the Management of Health Records.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No
Please list any other policies that are related to or referred to as part of this analysis	The Health and Social Care Act 2012 The Human Rights Act 1998 Caldicott 2 Principles –To Share or Not to Share? The Information Governance Review April 2013 Common Law Duty of Confidentiality NHS Care Records Guarantee for England HSCIC Guide to Confidentiality in Health and Social Care Access to Health Records Act 1990 Records Management Code of Practice for Health and Social Care 2016

	NHS Act 2006 Public Records Act 1958 The Data Protection Act 2018 The General Data Protection Regulation (GDPR).
Who will the policy, project or function affect?	All staff employed by or on behalf of Hull CCG.
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation has taken place locally.
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	The policy does not directly promote inclusivity but provides a framework for the CCG's approach to the Management of Health Records within the workplace, ensuring staff are supported by management and health professionals.

Equality Data		
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external	Yes	
	No	x

information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?
(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

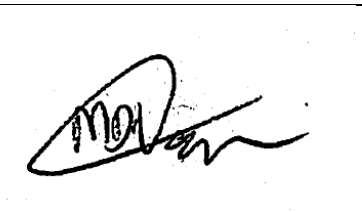
Protected Characteristic:	Neutral Impact:	Positive Impact:	Negative Impact:	Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.				
Gender	X			This policy applies to all regardless of gender.
Age	X			This policy applies to all regardless of age.
Race / ethnicity / nationality	X			This policy applies to all regardless of race/ethnicity/ nationality.
Disability	X			This policy applies to all regardless of

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

				disability.
Religion or Belief	x			This policy applies to all regardless of religion or belief.
Sexual Orientation	x			This policy applies to all regardless of sexual orientation.
Pregnancy and Maternity	x			This policy applies to all regardless of pregnancy/ maternity.
Transgender / Gender reassignment	x			This policy applies to all regardless of transgender/ gender reassignment.
Marriage or civil partnership	x			This policy applies to all regardless of marriage or civil partnership.

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
It is recognised that this Policy is written in English and there is therefore a risk to the staff whose first language is not English for misunderstanding.	The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language.	CCG Communications	Updating of this facility is ongoing.	Next Policy Review – November 2020.

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs

I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:
 **Signed:**
Date: 16.12.19