NHS
Scarborough and Ryedale
Clinical Commissioning Group

Corporate Records Management Policy, Standards and Procedural Guidance
November 2017

Authorship:	Information Governance Manager (eMBED)			
Committee Approved:	Audit and Governance Committee			
Approved date:	November 2017			
Review Date:	November 2020			
	Relevant	Screening	Full / Completed	Outcome
Equality Impact Assessment	Yes	Yes	No	No issues identified
Sustainability Impact Assessment	Yes		No	No issues identified
Privacy Impact Assessment	No	No	No	Not Relevant
Bribery Checklist	No		No	Not Relevant
Target Audience:	All CCG Staff			
Policy Reference No:	P707			
Version Number:	V4			

Publication/Distribution	Website	Email Staff	Others (i.e. SBC)
	Yes	Yes	No

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

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 & Date	Date on Intranet
0.1	H Sanderson	First Draft		
0.2	C Wallace	Updates and formatting corrections		
1.0	M Mason	Reformatted to CCG policy template	SMT Dec 2013	
2.0	H.Sanderson	Review against IGT V12 Addition of Data Quality Requirements. Update of Roles and Responsibilities Addition of non-compliance to the standard	Senior Management Team November 2014	
2.1	H. Sanderson	Reviewed ahead of planned review date no amendments required but review date reset for Sept 2017	IGSG October 2015	
3.1	H. Sanderson	Change of CSU references to Embed Health Consortium To Reference the Records Management Code of Practice for Health and Social Care 2016 Update types and formats of records detailed in Annex B covered by this policy and reference to guidance on how to deal with different types of records in the Code of Practice. Update to responsibilities Addition of compliance		

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
		to IG Toolkit Update to retention of records to include reviewing for continued retention at Annex K Update of the requirement to audit records annually at Annex M. Updates to the practice of scanning records at Annex E. Addition of guidance re Cloud based storage solutions and Digital Records at Annex E.		
4.0	IG Officer	Updates to reflect General Data Protection Requirement Updated for Changes in Relationship to Embed	November 2017	November 2017

Approval Record

Applicable Y/N	Committee / Group	Consultation / Ratification	Date taken to group	Date last Approved
	Governing Body	Ratification		
	Council of Clinical Representatives	Ratification		
Yes	SMT	Ratification	August 2014	August 2014
	Remuneration Committee	Ratification		
Yes	Audit and Governance Committee	Ratification	November 2017	November 2017
	Finance and Contracting Committee	Ratification		
	Business Committee	Ratification		
	Communications and Engagement Committee	Ratification		
	Quality and Performance Committee	Ratification		
	Primary Care Co-Commissioning Committee	Ratification		
	Other	Ratification		
	All Employees	Consultation		
	Public	Consultation		
	Yorkshire and Humber Social Partnership Forum	Consultation		

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 Code of Practice for Health and Social Care 2016 was published by the Information Governance Alliance as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS and Social Care 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 organisations 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 Records Management Code of Practice for Health and Social Care 2016.

2 ENGAGEMENT

This policy has been developed in line with national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

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

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify any benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors 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 1998 (DPA) and General Data Protection Regulation 2016, 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.

5 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.

Term	Definition
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.

Term	Definition
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.

6 POLICY PURPOSE AND AIMS

6.1 Organisational Standards

A register of organisational information assets is maintained and kept up to date– 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 individual 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 Code of Practice for Health and Social Care 2016, and the following legislative and professional requirements:-

- Data Protection Act 1998
- General Data Protection Regulation 2016
- 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
- Information Governance Toolkit

6.2 Records Management Procedure

6.2.1 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, 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(data) flows;
- the Information Asset Owner and the Information Asset Administrators for each information asset;
- information security measures put in place; and
- Business continuity plans.
- Retention Periods of each type of record registered
- Reference to the Records Management procedure for the information asset

This register must be reviewed annually by the departmental Information Asset Owner See Annex D

6.2.2 Data Quality

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.

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.

6.2.3 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 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.

6.2.4 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 for Health and Social Care 2016 sets out minimum statutory retention periods for key corporate documentation which must be followed. The retention period must be recorded on the Information Asset Flows of personal identifiable information *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*

6.2.5 Incident Reporting

All incidents and near misses relating to a breach in information security must be reported using the organisation's incident reporting system within 24 hours on the CCG reporting system to enable it to be reported on the IG Toolkit reporting system within 72 hours of being identified.

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 organisations Serious Incident Policy. The organisations Information Governance Manager must be informed. These must be reported to the SIRO and the CCG Management Team.

Any suspected thefts must be reported to the Police, by the individual responsible for the records at the time and noted on the organisations 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 Manager, Local Security Management Specialist,), to investigate such incidents and identify any learning points that must be implemented in order to prevent a recurrence.

6.2.6 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.

7 ROLES, RESPONSIBILITES AND DUTIES

Records management should be recognised as a specific corporate responsibility within the CCG. It should provide a managerial focus for records of all types and formats, including electronic records throughout their lifecycle.

A designated member of staff with appropriate seniority should have responsibility for records management within the CCG and this should be communicated throughout the organisation.

7.1 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 Records Management Code of Practice for Health and Social Care 2016 has been developed as a guide for NHS and Social Care organisations from which this policy has been produced.

7.2 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.

7.3 Roles/Responsibilities and Duties:

7.3.1 Chief Officer

Overall accountability for records management across the organisation lies with the Chief 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

7.3.2 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.

7.3.3 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.

7.3.4 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 Embed Health Consortium 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.

7.3.5 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. All records identified must be recorded on the CCG Information Asset Register and where records involve the processing of personal identifiable information these must be data flow mapped

7.3.6 Staff

All Staff are responsible for the records they create or use in the course of their duties and 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.

8 IMPLEMENTATION

This policy will be published on the CCG website and all staff will be made aware of its publication through communications and team meetings.

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'.

9 TRAINING AND AWARENESS

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

All staff, including temps and agency staff, students and any other personnel that may be required to use system 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.

A training module in respect of Records Management is available via the Information Governance Training Tool.

However all staff should also be made aware of the local records management procedures in respect of systems they will use to perform their duties.

10 NON-COMPLIANCE WIH THE STANDARD

Non- compliance 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

11 MONITORING AND AUDIT

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.

12 POLICY REVIEW

The policy and procedure will be reviewed at least every three years by the CCG in conjunction with managers, and Trade Union representatives if appropriate, with changes made as required and the outcome published. Where review is necessary due to legislative change, this will happen immediately.

These procedures will be retained in line with the Records Management Code of Practice for Health and Social Care 2016 retention schedules

Audit and Governance Committee has delegated responsibility for monitoring and reviewing the policy and will report any concerns to the Governing Body.

13 REFERENCES AND ASSOCIATED DOCUMENTATION

- Data Protection Act 1998
- General Data Protection Regulation
- 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

14 APPENDIX ONE – EXAMPLES OF RECORDS AND FORMATS

Examples of Records and Formats that should be managed in line with the Records Management Code of Practice for Health and Social Care 2016

Functions:

- Patient Health Records of all types (electronic or paper based), See section 3 of the Records Management Code of Practice for guidance on specific types on health records
- Letter to and from other health professionals
- Laboratory reports
- Printouts from monitoring equipment
- X-ray and Imaging reports, photographs and other images.
- Administrative Records including:
- 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).
- 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.
- Data Processed for secondary purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or supporting commissioning decisions.

The Records Management Code of Practice for Health and Social Care Section 3 provides further guidance on how to deal with specific types of records. Format:

- Photographs, slides or other images.
- Microfilm
- Audio and video tapes, cassettes, CD-ROM
- Emails
- Computerised Records
- Scanned Records
- Text Messages and Social Media
- Websites and Intranet Sites

This list is not exhaustive.

15 APPENDIX TWO – LEGAL AND PROFESSIONAL REQUIREMENTS

- Records Management Code of Practice for Health and Social Care 2016
- Data Protection Act 1998 & General Data Protection Regulation 2016
- 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

16 APPENDIX THREE - REGISTRATION OF RECORDS MANAGEMENT SYSTEMS

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 Code of Practice for Health and Social Care 2016. 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 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 Code of Practice for Health and Social Care 2016 and any organisational additions require registration.

17 APPENDIX 4 – 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.

17.1 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.

17.2 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.

17.3 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 Records Management Code of Practice for Health and Social Care 2016.
- Be stored in a manner that conforms to Health and Safety Policy.
- Be stored in a manner to prevent deterioration or loss.

17.4 Non-Current Records

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

The Records Management Code of Practice for Health and Social Care 2016 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, the requirements of the Data Protection Legislation.

17.5 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 these records i.e. in a lockable container and placed somewhere secure within the home.

17.6 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 Embed Health Consortium 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 mobile 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.

17.7 Other Media

17.7.1 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.

17.7.2 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 consent to the use of visual and audio recordings, an photographs must be recorded in an appropriate manner by the CCG.

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.

17.7.3 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.

The main consideration when scanning is to ensure that the information can perform the same function as the paper counterpart did and that like any evidence, scanned records can be challenged in court. Further guidance to the practice of scanning records in the Records Management Code of Practice for Health and Social Care 2016.

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.

17.8 Cloud Based Storage of Records

The use of cloud based solutions for health and social care is increasingly being considered. Before any cloud based solution is implemented there are a number of

considerations that must be taken into account. The Information Commissioners Office has issued guidance on cloud based storage and they also advice that a privacy impact assessment is conducted.

Further guidance as to the use of cloud storage is detailed in the Records Management Code of Practice for Health and Social Care 2016.

17.9 Digital Records, Digital Continuity, Digital Preservation and Forensic Readiness

The main issue with digital records is to ensure that the authenticity, reliability, integrity and usability of the records held is maintained over time.

Further guidance on the maintenance of digital records is detailed in the Records Management Code of Practice for Health and Social Care.

19 APPENDIX 4 – CREATION AND MAINTENANCE OF RECORDS STRUCTURES

19.1 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.

19.2 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.

19.2.1 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.

19.2.2 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).

19.2.3 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.

19.2.4 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.

.

20 APPENDIX FIVE - 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.

20.1 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

20.2 Personal Data

Under the requirements of DPA – Part II, Section 7, 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.

21 APPENDIX SIX – PROTECTIVE MARKING SCHEMA

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.

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 ad 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.

22 APPENDIX SEVEN - 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.

22.1 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.

22.2 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 to update otherwise the system will quickly be rendered ineffective.

22.3 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.

24 APPENDIX EIGHT – TRANSPORTING RECORDS

This section covers transport between:

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

24.1 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.

24.2 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.

Further guidance is available at:
https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/NHS%20IG-Secure%20Transfers%20of%20Personal%20Data%20Guidance-SupplementaryReqGuidance.pdf

24.3 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 lockable container or folder, and in an encrypted format where held electronically. These measures will help provide appropriate protection from damage, unauthorised access, such as or theft or loss.

24.4 Handling Records

The following rules must be applied when handling records

- Staff should never smoke near records and must take great care if eating or drinking whilst using records as spillages could cause information to be damaged or lost.
- Records containing personal confidential information being carried on-site, e.g. from the archive storage to the department, etc. should never 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 mobile 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 lockable container.

24.5 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 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.

26 APPENDIX NINE - RECORDS RETENTION AND REVIEW

26.1 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; see Schedule 1, Part 1, and Principle 5 of the Data Protection Act 1998. The General Data Protection Regulation also requires that the retention period of each data flow of personal identifiable information is recorded on the data flow map.

The organisation has adopted the retention periods for health and non-health records as set out in the Records Management Code of Practice for Health and Social Care 2016 as detailed in Appendix Three of the Code.. The retention schedule will be reviewed annually by the Records Manager, and maintained in accordance with the Records Management Code of Practice for Health and Social Care 2016. Evidence of this process and communication of relevant up dates will be reported to the Information Governance Steering Group.

It should be noted that the retention periods given in the Appendix 3 schedule to the Code of Practice are minimum periods. The CCG must have a process in place to decide when records need to be retained for longer than the minimum period, were records are required to support on-going FOI or public enquiries. Further guidance is available in the Code of Practice under Review for continued retention.

The retention of records for longer than the recommended period must be discussed with the organisations 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 areas. 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.

27 APPENDIX TEN – 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.

27.1 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 and clauses, refer to the Information Governance Manager for details.

27.2 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 IMT Department to ensure that all records to be destroyed are done securely.

28 APPENDIX ELEVEN - 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.

35 APPENDIX TWELVE – AUDIT OF RECORDS MANAGEMENT SYSTEMS

The organisation should annually complete a survey or audit of their records to ensure they understand the extent of their records management responsibilities. See Audit of Records/ Information Asset Management in the Code of Practice for further guidance

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:

35.1 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 at out 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.

35.2 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. It is also required that the retention period of each type of record is determined and recorded on the data flow map. 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.

36 APPENDIX THIRTEEN – 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.	Appendix 3 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	Appendix 4	
4.	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, data quality and retention periods of records, this applies to both manual and electronic systems	Appendix 5	
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.	Appendix 6	
6.	Protective Marking Schema.	This indicates of the confidential nature of each document or record and informs staff of the	Appendix 7	

No.	System Requirement	Description	Guidance Reference	Complete Y/N
		appropriate level of care and confidentiality with which the document or record should be treated.		
7.	Tracking and Tracing	This facilitates a mechanism by which the location of records or copies of records can be known at all times.	Appendix 8	
8.	Transporting and Transferring Records	The transportation of records, documents and all portable media containing records must be transported securely.	Appendix 9	
9.	Records Retention and Review	The Records Management Code of Practice for Health and Social Care 2016 sets out statutory retention periods for key corporate documentation which must be followed. This must be recorded on data flow maps	Appendix 10	
10.	Secure Records Disposal	All records must be disposed of in a secure manner to render the information illegible and non-retrievable.	Appendix 11	
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.	Appendix 12	

38 APPENDIX FOURTEEN – EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Strategy Policies

General Information		
Policy:	Corporate Records Management Standard	
Date of Analysis:	November 2017	
Policy Lead: **(Name, job title and department)**	Information Governance Manager (eMBED)	
What are the aims and intended effects of this policy?		
Are there any significant changes to previous policy likely to have an impact on staff, patients or other stakeholder groups?	None	
Please list any other policies that are related to or referred to as part of this analysis	None	
Who is likely to be affected by this policy?	General Public	☐
	Service Users	☐
	Staff	☒
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Not applicable	
Promoting Inclusivity and NHS Scarborough and Ryedale 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	Not applicable	

Equality Data

Age

Data provided below is from Census 2011

Age Range	Number	%
0-14	17,672	14.9
15-44	39,530	33.2
45-64	15,427	13.0
65-74	9,083	7.6
85+	3,820	3.2

Gender

JSNA 2016

	%
Male Residents	49.6
Female Residents	50.4

Race / Nationality

BME – 2011 Census Data

	%
White	97.5
Mixed	0.8
Asian	1.2
Black	0.2
Other	0.2

Languages – 2011 Census Data

	%
English	97.5
Polish	0.8
Other EU Language	0.6
Other	1.86

Gypsy and Travellers – 2011 Census Data

Scarborough	37
Ryedale	81

Disability

2011 Census Data

	%
Long Term Health Problem/Disability	21.3
Limiting Long Term Illness	20.4

Projecting Adult Needs and Service Information (PANSI)-2017 Estimates

	Scarborough	Ryedale
Limiting Long Term Illness - day to day activities limited a little	7,507	3,455
Limiting Long Term Illness - day to day activities limited a lot	6,513	2,462
Mobility - unable to manage at least one activity on their own	5,210	2,509
Learning Disability – Including Down's syndrome	947	469
Learning Disability – Autistic Spectrum Disorders and Down's Syndrome	81	134
Visual Impairment - Moderate or severe	3,323	1,588
Hearing Impairment – some hearing loss	17,167	8,370
Hearing Impairment – Moderate or Severe	2,215	1,070
Dementia	1,973	959
Depression	2,474	1,585
Learning Disability – Baseline	1,454	708
Learning Disability – Moderate - Severe	415	1,128
Learning Disability – Autistic Spectrum Disorders	592	289
Learning Disability – Down's syndrome	38	18
Physical Disability – Moderate	5,176	2,620
Physical Disability – Serious	1,605	824
Physical Disability – Personal Care	3,198	1,639
Visual Impairment – Serious	39	19
Hearing Impairment – Some hearing loss	69,328	3,565
Hearing Impairment – Severe	395	203
Mental Health Problems	4,331	2,096

Sexual Orientation

In relation to sexual orientation, local population data is not known with any certainty. In part, this is because until recently national and local surveys of the population and people using services did not ask about an individual's sexual orientation. However, nationally, the Government estimates that 5% of the population are lesbian, gay or bisexual communities.

Gender Reassignment

There are not any official statistics nationally or regionally regarding transgender populations, however, GIRES (Gender Identity Research and Education Society - www.gires.org.uk) estimated that, in 2007, the prevalence of people who had sought medical care for gender variance was 20 per 100,000, i.e. 10,000 people, of whom 6,000 had undergone transition. 80% were assigned as boys at birth (now trans women) and 20% as girls (now trans men). However, there is good reason, based on more recent data from the individual gender identity clinics, to anticipate that the gender balance may eventually become more equal.

Religion / Belief

2011 - Census Data

	%
Christian	67
Buddhist	0.3
Hindu	H0.1
Jewish	0.1
Muslim	0.5
Sikh	0.1
Other Religion	0.4
No Religion	24.3
Religion not stated	7.4

Pregnancy and Maternity

	Live Births (ONS 2016)	Still Births (ONS 2016)
Scarborough	1,034	4
Ryedale	439	2

Marriage and civil partnership

Data provided below is from Census 2011

	Number	%
Single	32,890	28.2
Married	57,934	49.7
In registered same sex civil partnership	259	0.2
Separated (incl civil partnership)	2,866	2.5
Divorced (incl civil partnership)	12,043	103
Widowed	10,486	9

This protected characteristic generally only applies in the workplace.

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:	No 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)
Gender	X			
Age	X			
Race / ethnicity / nationality	X			
Disability	X			
Religion or Belief	X			
Sexual Orientation	X			
Pregnancy and Maternity	X			
Transgender / Gender reassignment	X			
Marriage or civil partnership	X			

What sources of equality information have you used to inform your piece of work?
(Please refer to the JSNAs and Population data, previous engagement findings, research, patient experience reports etc.)

Not applicable

What measures have been put in place to mitigate any potential impact?

Not applicable

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

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:

Sign-off

All EIAs must be signed off by a member of SMT
I agree with this assessment / action plan
Signed off by (Name/Job Title)
Signed: Sally Brown
Date: November 2017

39 APPENDIX FIFTEEN – SUSTAINABILITY IMPACT ASSESSMENT

SUSTAINABILITY IMPACT ASSESSMENT

Instructions

Sustainability is one of the CCG's key priorities and consequently the CCG has made a corporate commitment to address the environmental effects of its activities across all service areas. The purpose of the Sustainability Impact Assessment is to record any positive or negative impacts that a Policy / Board Report / Committee Report / Service Plan / Project is likely to have on each of the CCG's sustainability themes. The Sustainability Impact Assessment enables any relevant impacts to be identified and potentially managed.

The Sustainability Impact Assessment is based on assessing the impact of the activity against a series of criteria covering environmental sustainability issues. It would be most desirable for activities to score positively in as many areas as possible, although it is likely that some areas will score positively against some themes, and negatively against others.

Using the Sustainability Impact Assessment template

To complete the Sustainability Impact Assessment template, you should consider whether the Policy / Board Report / Committee Report / Service Plan / Project will have a positive or negative impact on each of the themes by placing a mark in the appropriate column. When you think there is likely to be an impact, please provide some annotations regarding the nature of the impact, and any actions that will be taken to address that impact. Users should note that not every theme will be relevant. Where this is the case the 'No Specific Impact' column should be marked. Users should also consider the following tips:

1. Make relative not absolute judgements (e.g. a new energy efficient service would score positively even if it consumes more energy than if no service were provided).
2. Be aware that small positive changes could be outweighed by negative ones (e.g. new energy efficient lighting in the short term may outweigh the benefits of maintaining current lighting).
3. If there are both positive and negative impacts, these need to be recorded in order to give a balanced view. Be objective and unbiased.
4. Concentrate on the most key significant issues - there is the potential to consider the appraisal in a very detailed way. This should be avoided at this stage.
5. Judge a proposal over its whole lifespan and remember that some impacts may change over different timescales.

If you require assistance in completing the Sustainability Impact Assessment please contact the Corporate Services Team

Domain	Review questions	Assessment of Impact Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
Models of Care	Will it minimise 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes? Will it create incentives to promote prevention, healthy behaviours, mental wellbeing, living independently and self-management? Will it provide evidence-based, personalised care that achieves the best possible health and well-being outcomes with the resources available? Will it reduce avoidable hospital admissions or permanent admissions to residential care or nursing homes? Will it pay for services based on health outcomes rather than activity for example through personal budgets? Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways? More info: http://www.sduhealth.org.uk/areas-of-focus/clinical-and-care-models.aspx	n/a		
Travel	Will it reduce 'care miles' (telecare, care closer) to home? Will it reduce repeat appointments? Will it provide / improve / promote alternatives to car based transport (e.g. public transport, walking and cycling)? Will it support more efficient use of cars (car sharing, low emission vehicles, community transport, environmentally friendly fuels and technologies)? Will it improve access to services and facilities for vulnerable or disadvantaged groups or individuals? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/travel.aspx	n/a		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/waste.aspx Will it reduce water consumption? Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)? Will it improve green space and access to green space? More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/energy.aspx	n/a		

Adaptation to Climate Change	Will it support mitigation of the likely effects of climate change (e.g. identifying proactive and community support for vulnerable groups; contingency planning for flood, heatwave and other weather extremes)? More info: http://www.sduhealth.org.uk/areas-of-focus/community-resilience/community-resilience-copy.aspx	n/a		
Procurement	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery in line with the Public Services (Social Value) Act 2012? Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives? Will it reduce waste, environmental hazards and toxic materials for example by reducing PVC, antibiotic use, air pollution, noise, mining and deforestation? Will it reduce use of natural resources such as raw materials, embedded water, and energy to promote a circular economy? Will it support the local economy through local suppliers, SMEs or engage with third sector or community groups? Will it promote ethical purchasing of goods or services e.g. increasing transparency of modern slavery in the supply chain globally? More info: http://www.sduhealth.org.uk/areas-of-focus/commissioning-and-procurement/procurement.aspx	n/a		
Workforce	Will it provide employment opportunities for local people? Will it promote or support equal employment opportunities? Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)? Will it offer employment opportunities to disadvantaged groups and pay above living wage? More info: http://www.sduhealth.org.uk/areas-of-focus/social-value.aspx	n/a		
Community Engagement	Will it promote health, increase community resilience, social cohesion, reduce social isolation and support sustainable development? Will it reduce inequalities in health and access to services? Will it increase participation including patients, the public, health professionals and elected officials to contribute to decision making? Have you sought the views of our communities in relation to the impact on sustainable development for this activity? Will it increase peer-support mechanisms? More info: http://www.sduhealth.org.uk/areas-of-focus/community-resilience.aspx	n/a		
Estimated carbon benefit	What is the estimated carbon benefit (in terms of tCO_2e) from the implementation of this project? As opposed to the current business as usual position. Speak with your sustainability manager and see the following guidance: More info: http://www.sduhealth.org.uk/areas-of-focus/carbon-hotspots/pharmaceuticals/cspm/sustainable-care-pathways-guidance.aspx	n/a		

40 APPENDIX SIXTEEN – PRIVACY IMPACT ASSESSMENT

Privacy Impact Assessment (PIA)

Screening Questions

The below screening questions should be used inform whether a PIA is necessary. This is not an exhaustive list therefore in the event of uncertainty completion of a PIA is recommended.

Please contact the Corporate Services Team of IG Manager (eMBED) if you need any assistance

Project title	Corporate Records Management Standards
Brief description	

Screening completed by

Name	Emma Parker
Title	Corporate Services Manager
Department	Corporate Services
Telephone	01723 343691
Email	Emma.parker6@nhs.net
Review date	November 2017

Marking any of these questions is an indication that a PIA is required:

	Screening Questions	Tick
1	Will the project involve the collection of identifiable or potentially identifiable information about individuals?	☐
2	Will the project compel individuals to provide information about themselves? i.e. where they will have little awareness or choice.	☐
3	Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?	☐
4	Are you using information about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development.	☐
5	Where information about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people would consider to be sensitive and private.	☐
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	☐
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	☐
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition or automated decision making.	☐

Please retain a copy of this questionnaire within your project documentation.

If you have ticked any of the questions above – please complete a full Privacy Impact Assessment – The most up to date version of the form is available on the CCG website at:

http://www.scarboroughryedaleccg.nhs.uk/publications/policies-2/