Document information

Document type:	Policy
Document reference:	
Document title:	**Records Management Policy**
Document operational date:	March 2014
Document sponsor:	David Noyes, Director of Planning, Performance and Corporate Services
Document manager:	Susannah Long, Governance & Risk Manager
Approving Committee/Group:	Audit & Assurance Committee
Approval date:	March 2017
Version:	3.0
Recommended review date:	March 2020
Internet location:	Intranet only – Policies section

Please be aware that this printed version of this document may NOT be the latest version. Please refer to the internet for the latest version.

Summary

This policy has been created to detail the requirements for creating, managing and using corporate records appropriately in accordance with relevant legislation and codes of practice.

Consultation

This policy was developed in consultation with South Central and West Commissioning Support Unit (SCW CSU) and has been agreed by the CCG Information Governance Group.

Appendices

The following appendices form part of this document:

Appendix 1:   Key Records Management Statutory and NHS Requirements
Appendix 2:   NHS Wiltshire CCG Records Framework

Version Control (change record and reviewers/contributors)

Version	Date	Reviewed by:	Page	Reason for Change	Changes approved by:	Approval date:
1	April 2015	Records Manager, CSCSU; Governance & Risk Manager CCG; Information Governance Group (IGG) CCG		Introduction of Manual; Reshaping of policy for clarity; Removal of CCG Records Management Group; Review of information assets from six months to annually; Reference to TNA; Retention Schedule and Auditing Standard will now be included as part of the records management manual; WCCG Records Framework now detailed at App2	Audit & Assurance Committee	May 2015
V2.2	Feb 2017	SCW Records Manager; Governance & Risk Manager CCG; IGG	5	Add ISO and DPA Record definition.	Audit & Assurance Committee	March 2017
			5, 6	CCG Corporate Records and Clinical Records – define (declare) a record.		
			9	BS 10008 standard for scanning documents.		
			9	Referenced NHS England 5 year plan.		
			9	Updated to: Records Management Code of Practice for Health and Social Care 2016		
			10,11 &12	Records Security and Access updated in line with NHS England and Government security classification		
			13	Email – updated.		
			15	Corporate Records update.		
			16	1958 added.		
			18	Update with new Code of Practice.		
			19	Update with new Code of Practice.		
			All	Add: Classification: OFFICIAL		

Acknowledgements

RECORDS MANAGEMENT POLICY

1.0   INTRODUCTION AND PURPOSE

Records management is the process by which the CCG manages the records it creates. Information is a corporate asset and it is important that records are created in a standard and consistent manner.

This policy details all aspects of records management, from creation through to disposal. It is important that records are filed and stored appropriately so they are accessible when needed.

Adherence to this policy will ensure that the CCG meets its data protection legal requirements, records management standards, and other relevant information and corporate governance requirements.

The purpose of this document is to set out a framework for the management of corporate records created and used within NHS Wiltshire CCG. It is supported by a procedure and guidance manual that must also be consulted. The application of a disciplined approach to Information and Records Management practice is a key corporate discipline and responsibility. The purpose of this is to ensure that:

- Decisions are recorded appropriately
- Decisions are made based on accurate high quality information
- Organisational corporate memory is retained and evidence can be found to support decisions
- Reduced time wastage trying to find information
- Information can be located for audit and assessment purposes
- Better use of physical and server space
- Better use of staff time
- Improved control of valuable information resources
- Compliance with legislation and standards
- Reduced costs

Good records and the management thereof also avoids unnecessary duplication of work, and provides a sound basis for future work, analysis or audit. They will also allow the CCG to justify or explain actions in the future, comply with national legislation and demonstrates transparency. Having the right information at the right time is critical to good decision making.

2.0   SCOPE AND DEFINITIONS

2.1   Scope

This policy applies to all directly and indirectly employed staff, both permanent and temporary, working with NHS Wiltshire CCG.

2.2   Definitions

ISO 15489-1:2016 Information and documentation - Records management Records Lifecycle – defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses. (Source: Records Management Code of Practice for Health and Social Care 2016).

The Data Protection Act 1998 (DPA) S68(2) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

CCG Corporate Records and Clinical Records

We define (declare) a record as:
- any form of information which has been created or gathered as a result of any aspect of our work.
- finalised/completed evidence of our work. For example, draft polices of 0.4, 0.5 would be working documents; version 1.0 (final) would be the record.
- assigned the correct data classification
- original and unique
- information assets that we wish to retain for defined periods of time because they have a value to the organisation
- being manual (paper) and, most commonly, electronic in format. Examples include invoices, reports, audits, analysis, email correspondence, faxes, contracts, photographs, pictures, datasets, websites, social media and spreadsheets.

As a general rule, what should not be considered as records includes:
- work-in-progress / draft documents, temporary notes intended to be typed up, copies / duplicates of existing records, reference copy print-offs, private / non-work information, CC'd / BCC'd emails, publicity or circular material. This information should not be retained for extended periods. Best practice would be to undertake a robust cleansing exercise and dispose or delete.

All records, including those of customers, are the property of the NHS and are Public Records as defined by the Public Records Act 1958.

All recorded information is in the scope of this policy because whatever it's perceived value or status as a record, it may still be used to support litigation or requests for information e.g. Freedom of Information, Subject Access Requests.

Another organisation's records are also in scope as they can support our activities and may need to be retained by us for a period of time.

This policy covers all CCG business areas and record formats.

'**Records Management**' is the process by which an organisation manages all the aspects of records from their creation, through to their eventual disposal.

3.0   PROCESS/ REQUIREMENTS: RECORDS MANAGEMENT COMPONENTS and PRINCIPLES

3.1 Information Lifecycle Management

Information lifecycle management is the approach to managing corporate information within the CCG. This covers the following five areas:

Lifecycle Stage	Description
1. Planning	At a corporate level we shall develop and implement policy, procedures and functionality to deliver compliant records management. Our departments shall ensure they have identified key records that must be captured as a result of their activities and that these are managed following policy.
2. Creation & receipt	This is where a record is created and is saved. Records must be accurate, filed appropriately and access controlled where necessary (for example HR records only accessible by designated managers). Any information is named following the agreed standard.
3. Use / Distribute	Our records shall be appropriately available so that they support current business and decision making as well as statutory access requirements. Wherever possible we shall share one version of records rather than create duplicates. Records must be used in accordance with the Data Protection Act (DPA) principles and version control used as appropriate. Where business reasons dictate that records need to be taken off site, the records must be adequately protected at all times.
4. Retention	We shall retain non-current and superseded records in our filing system so to support ongoing business needs and compliance requirements. Our disposal schedules shall govern how long records are retained. Retained records shall continue to be protected and accessible with storage facilities meeting appropriate standards.

Lifecycle Stage	Description
5. Disposal	Our records shall not be retained indefinitely. At the end of the retention, records shall be disposed of. In most cases this will mean controlled destruction; a small percentage of records may become archive meaning that they will be retained indefinitely under the Public Records Act.

3.2 Good Quality Records

Our records are evidence of our activities. They may be required for litigation, audits, statutory enquiries and as a basis for decision making. Our records need to be of good quality, accurate, unambiguous, concise, clear, consistent and timely, and in a form which we can access and exploit. Managers shall be clear on what records are required to sufficiently document business activities, and ensure that staff capture them following policy and procedure.

The quality and accuracy of records that relate to patient care and significant changes to services and policy are particularly important.

3.3 Manual / paper records

In keeping with wider NHS agenda (NHS England Five Year Forward Plan), the CCG will endeavour to maintain records electronically, where practicable. Original electronic records will be considered the primary version. Paper copies of electronic records should be maintained by exception and shall be appropriately destroyed at the earliest convenience.

Where it is practical to do so, the CCG will scan new or legacy paper records following the scanning guidance (this follows standard BS 10008 so to protect legal admissibility of scanned paper records. The original copies of scanned records must then be securely destroyed.

In some cases it might be desirable to hold original ink signed records. This is permissible, although scanning such documents is acceptable so long as their legal admissibility has been protected by following the scanning guidance.

Any paper records we hold shall be securely held in appropriate local filing cabinets. Significant collections of closed manual records shall be stored with our paper record storage company.

Original paper records will be tracked if they are moved from their normal storage location. A log will be kept which includes a reference, description of the record, who has possession of the item, the date of removal and the date of return.

3.4 Disposal Schedules and Legal Holds

We shall not retain all of our records indefinitely. Disposal is the process that leads to records being destroyed or transferred elsewhere.

Our records shall be retained and disposed of following agreed disposal schedules and procedures that are based on Records Management Code of Practice for Health and Social Care 2016 and business needs. Our disposal schedules are approved by the Senior Information Risk Officer (SIRO) and the Information Governance Group (IGG). **Disposal shall always be carried out following confidentiality and sensitivity requirements.**

Be aware – you should not destroy any records where a request for information has already been received. If a record due for destruction is known to be the subject of a request, the destruction should be delayed until disclosure has taken place, or the relevant appeals process has been completed should the record be withheld.

3.5 Record Naming

CCG electronic records along with holding folders shall be named following the agreed electronic document naming standard. This shall also include version controls so that it is clear what the status and iteration of the record is.

3.6 Accredited File Shares

CCG electronic records shall be saved to our approved and governed file shares (if not already saved to a database see below) and include folders that assist with disposal management and protection of sensitive information.

As a general rule, original electronic records shall not be saved to 'offline' storage such as internal PC hard drives, USBs or optical media. In some circumstances e.g. anticipated limited network connection, staff may need to save copies of records to encrypted devices e.g. USB memory stick, Laptop internal hard disk. This is permissible if acceptable use policy is followed, and any new records / versions are saved to the approved 'online' storage location as soon as possible and subsequently deleted from the storage device.

The CCG also needs to be able to find and retrieve documents easily and quickly, at all times mindful of protecting confidential information.

3.7 Line of Business Systems / Databases

Many of our records are held within databases. These may be in the form of uploaded documents e.g. a PDF or email, or as data streams, e-transactions and system actions. This policy applies to these records. System owners and project managers shall consider the requirements of this policy when implementing, procuring or using databases.

Electronic records that are uploaded to databases e.g. an email into Datix, should be deleted from local systems e.g. Inbox or File Share – it is bad practice to duplicate information across systems.

3.8 Records Security and Access

The 'new' Government Security Classifications were published in April 2014 and provide assistance on how to share and protect information. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats.

NHS England has issued guidance based on the Government Security Classification. The NHS England Documents and Records Management Policy V3.0 states:

Classification of NHS Information - Marking Guidance from NHS England 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.

Official – ALL routine public sector business, operations and services should be treated as OFFICIAL.

A limited subset, that incorporates a descriptor, will be used in the event of needing to control access to these records. The originator or Data Controller is responsible for identifying sensitive data within this category and must put in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements.

Please refer to the table below for further guidance:

Category	Definition	CCG Marking (including descriptor)
Appointments	Concerning actual or potential appointments not yet announced.	OFFICIAL-SENSITIVE: COMMERCIAL
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).	OFFICIAL-SENSITIVE: COMMERCIAL

Category	Definition	CCG Marking (including descriptor)
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.	OFFICIAL-SENSITIVE: COMMERCIAL
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts	Concerning tenders under consideration and the terms of tenders accepted.	OFFICIAL-SENSITIVE: COMMERCIAL
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.	OFFICIAL-SENSITIVE: COMMERCIAL
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).	OFFICIAL-SENSITIVE: COMMERCIAL
Patient Information	Concerning identifiable information about patients.	OFFICIAL-SENSITIVE: PERSONAL
Personal	Concerning matters personal to the sender and/or recipient CCG addition: Personal Record.	OFFICIAL-SENSITIVE: PERSONAL
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published)	OFFICIAL-SENSITIVE: COMMERCIAL
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff	Concerning identifiable information about staff.	OFFICIAL-SENSITIVE: PERSONAL

Please note that there is no need to apply the new classification procedure retrospectively.

Classifications must be in CAPITALS at the top of each page.

CCG records shall not be saved to private (home) computers nor shall private email e.g. Hotmail, be used to transmit our records or carry out NHS business. Home printers shall not be used to print CCG records.

Our Accredited File Shares shall include protected folders and permission protocols where sensitive records are held e.g. records containing personal data.

Access restrictions to records shall be proportionate; wherever possible, records should be available to all staff so to aid information sharing, and reduce duplication and risks.

3.9 Email Records / Electronic Communication

Email is a key communication. The email service is designed as a communication tool and is not an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or formal record of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden to your organisation and information may become difficult to locate due to the size of files and attachments being stored.

Particular attention must be paid to ensuring that emails relating to patients (clinical records) are dealt with promptly and were appropriate, deleted as the pertinent information has been transferred to the relevant record.

Staff shall regularly housekeep their Mailboxes so that transitory and spam type emails are deleted. Managers shall ensure all required email records are transferred from a leaver's Mailbox to the approved appropriate store.

Other forms of electronic communication such as Instant Messaging and video conferencing will likely become more commonplace – these 'recordings' if retained, qualify as records and so shall be managed under this policy. Additional policy / procedure will be produced as required.

3.10 Records Compliance Audit

The CCG will regularly audit records management practices across teams for compliance with this framework and the requirements of the Information Governance Toolkit around Corporate information assurance.

Staff are expected to comply with the requirements set out within this Records Management Policy and its supporting procedures. Non adherence to the records framework may result in disciplinary policies being implemented.

3.11 Inventory of Corporate records

The CCG needs to know what information it holds, where it is kept and how it is being used. A detailed inventory must be completed for all records stored on or off-site.

Having an inventory also assists with:
- managing retention, appraisal and disposal of records (Lifecycle of the record).
- Seeing where paper and electronic records are stored
- Assessing the general condition of stored records
- Obtaining an overview of the types of information held
- Determining if duplicate records exist
- Assessing current and future storage requirements
- Identifying any record creation / disposal concerns
- Identifying any information security concerns
- Support litigation or requests for information

The inventory of records (information assets) will be reviewed every year.

3.12 Reporting of records management incidents

The recent Caldicott 2 review concluded that serious clinical incidents in which any data management issue is identified should be reported in a similar manner to data breaches. Consequently, staff will be expected to refer to the CCG Adverse Event Reporting Policy for reporting arrangements.

4.0 ROLES AND RESPONSIBILITIES

4.1 All Staff

All NHS records are public records under the terms of the Public Records Act 1958, therefore, all NHS organisations have a duty to make arrangements for the safe keeping and eventual disposal of their records.

Records management is part of everyone's job. All staff, both permanent and temporary, must ensure that they comply with their records management responsibilities. Failure to comply with this policy may result in disciplinary action and/or civil/criminal action.

4.2 Information Asset Owners

Information asset owners (IAO) shall ensure that information risk assessments are performed at least every six months on all information assets where they have been assigned 'ownership', following guidance from the SIRO. This work will establish and, subsequently, review the records inventory.

IAO's will have overall responsibility for record keeping across their assigned information assets and for signing off record disposal / deletion requests.

4.3 Information Asset Administrators

Information Asset Administrators (IAA) shall manage the information held within a department in line with the Data Protection Act 1998 and CCG Information Governance policies. IAA will carry out information risk assessments as directed. IAAs will act as local records management experts and guide and advise colleagues on policy requirements, manage records disposal and liaise with the CSU Records Manager and CCG Records Management Lead as necessary.

IAAs and IAOs will be required to attend IG and / or records management workshops and training.

4.4 CSU Records Manager

The CSU will provide expert records management advice to the CCG on an on-going basis including the Information Governance Group.

4.5 CCG Records Management Lead

The CCG Governance & Risk Manager will act as the Records Management Lead for the CCG providing an interface with the CSU and advice to staff.

4.6 Records Management Lead Director

The Director of Planning, Performance and Corporate Services will act as accountable executive lead for records management.

4.5 Senior Information Risk Officer (SIRO) and Caldicott Guardian

The implementation of this policy as part of the general Information Governance agenda will be reviewed by the SIRO and Caldicott Guardian as it fits in with their specific roles.

4.6 Information Governance Group

The IGG will consider aspects of the records management agenda and will undertake an annual review of this policy.

5.0   TRAINING

Records management training is mandatory for CCG staff as laid out in the Training Needs Analysis (TNA). Additional training may form part of PDP dependant on role.

Induction	During their induction all new staff whether contractors or permanent shall be introduced to the basic principles of our records management policy and procedures.
Standard User	On an annual basis all staff shall complete this course to embed records keeping requirements and reinforce good practice.

6.0   EQUALITY, DIVERSITY AND MENTAL CAPACITY

An Equality Impact Assessment (EIA) has been completed for this policy and no adverse effect has been identified. The EIA will be published on the CCG internet.

This policy has been assessed and meets the requirements of the Mental Capacity Act 2005.

7.0   SUCCESS CRITERIA / MONITORING EFFECTIVENESS

It is important to ensure that the policy document achieves its aims and is adhered to by successful implementation and monitored outcome measures.

On an annual basis an audit to critically review the CCG assessment against the Information Governance Toolkit will be carried out by internal audit. Findings of this audit will be reported to the Audit & Assurance Committee. Implementation of any actions regarding records management that are identified as necessary or recommended during the audit will be monitored, as a minimum, at the next annual assessment.

In addition, the CCG Records Framework includes a compliance audit (Evaluation Standard) that will be used by the CCG Records Management Lead and by Directorates/Groups to assess compliance with this policy. Results from any corporate assessment will be presented to the Information Governance Group.

Any non-compliance with this policy should immediately be reported using the Non-compliance Form contained within the Policy on Management of Procedural Documents.

8.0   REVIEW

This document may be reviewed at any time at the request of either staff side or management, but will be reviewed where there is any major change in legislation or NHS guidance and on an annual basis.

9.0   REFERENCES

- The Health & Social Care Act 2012
- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;
- Records Management Code of Practice for Health and Social Care 2016
- Data Protection Policy

Key Records Management Statutory and NHS Requirements

Legislation / Standard	Compliance Requirement
Public Records Act 1958	All NHS records are Public Records. All NHS organisations must make arrangements for the safe keeping and disposal of their information and records. Recent changes have reduced the 30 year public records disposal rule to 20 years.
Freedom of Information Act 2000 including Section 46 Code of Practice for Records Management.	Provisions for disclosure of information held by public authorities. Includes a Records Management Code of Practice to support the Act which gives guidance on good practice in records management. It applies to all authorities subject to the Act, to the Public Records Act 1958 or to the Public Records Act (Northern Ireland) 1923.
Data Protection Act 1998	Regulates the processing of personal data relating to living persons. Principle 5 of the act notes the requirement not to retain data for longer than necessary – **records must be identified, consistently stored and have disposal schedules to meet Principle 5.**
Access to Health Records Act 1990	Regulates access to the records of a deceased person.
Records Management Code of Practice for Health and Social Care 2016	The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. The code includes records of staff, complaints, corporate records and any other records held in any format or media.

Appendix 2

NHS Wiltshire CCG Records Framework

Name	Purpose	How to find this document
Records Management Policy	Defines our approach to records and relevant rules. Scope includes all information types including email and line-of-business systems	Intranet
Records Management Strategy	Our longer term aims and objectives regarding records management for implementing our records framework.	Intranet
Records File Plan and disposal schedules	Our records taxonomy along with agreed disposal schedules.	Intranet
Records Procedures / Guidance	1. Understanding NHS Records 2. Scanning Records 3. Naming and version control of electronic documents 4. Using the File Share 5. Record Disposal Management 6. Handling Email Records 7. Security Classifications	Intranet
Compliance Audit	Improving records management maturity is dependent upon regular audits both in terms of compliance with policy but also inventories as of existing record stores.	Intranet
Training modules	To equip staff with the knowledge they need to effectively keep records or to manage the system. Training will be mandatory.	Intranet