

OFFICIAL



Records Management Policy

FINAL V4

NHS North Hampshire
Clinical Commissioning Group

DOCUMENT CONTROL

Document Name	Version	Status	Author
Records Management Policy	4	Final	South, Central and West Records Manager
Document objectives:	This policy sets out roles and responsibilities for records management and the key operating principles for record keeping and information lifecycle management across South, Central and West.		
Target audience:	All staff		
Committee/Group Consulted:	South, Central and West Information Governance Steering Group		
Monitoring arrangements and indicators:	This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.		
Training/resource implications:	All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet Information Governance page.		
Approved and ratified by:	South, Central and West Information Governance Steering Group	Date: 7 th June 2018	
	South, Central and West Corporate Governance and Assurance Group	Date: 25 th June 2018	
Equality Impact Assessment:	Yes	Date: January 2015	
Date issued:			
Review date:	April 2019		
Author:	South, Central and West Records Manager		
Lead Director:	Head of Information Governance		

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
04.09.17	Angela Oakley	V3.0 Draft GDPR Update	Throughout document	Draft amendments in line with Data Protection Bill and GDPR
17.04.2018	Rachel Lloyd	V3.1 Draft GDPR Update	Page 5 Throughout document	Include statutory and NHS guidelines Draft amendments in line with Data Protection Act 2018 (currently at Bill stage) and GDPR
26.04.2018	Angela Sumner	V3.1 Draft GDPR Update	Throughout document	Draft amendments in line with Data Protection Act 2018 (currently at Bill stage) and GDPR
14.05.2018	Arif Gulzar	V3.2	13	3.9 Data Backups – add Backup and Business Continuity Policy and shadow copies.

Reviewers/contributors

Name	Position	Version Reviewed & Date
Parveen Sharma	Equality and Diversity Lead	January 2015
Rachel Lloyd	SCW Records Manager	V2 13.01.2017
SCW Information Governance Steering Group		V2 10.01.2017
Rachel Lloyd	SCW Records Manager	V3.1 17.04.2018
Angela Sumner	Senior Information Governance Manager	V3.1 26.04.2018
Lucy Long	Information Governance Manager	V3.2 27.04.2018
Arif Gulzar	Cyber Security Manager	V3.2 27.04.2018
Beverley Carter	Head of Information Governance	V3.2 27.04.2018
Shelley Brown	Regional Information Governance & Records Management Lead	V3.2 27.04.2018

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

CONTENTS

Contents.....	4
1. INTRODUCTION.....	5
2. SCOPE AND DEFINITIONS.....	5
3. PROCESSES/REQUIREMENTS.....	6
4. ROLES AND RESPONSIBILITIES.....	15
5. TRAINING.....	16
6. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT.....	16
7. MONITORING COMPLIANCE AND EFFECTIVENESS.....	17
8. REVIEW.....	177
9. REFERENCES AND ASSOCIATED DOCUMENTS.....	178
Appendix 1: Key Records Management Requirements.....	19
Appendix 2: Clinical Records Guidance.....	21
Appendix 3a Protective Marking Scheme.....	23
Appendix 3b - Categories of data/information.....	29

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

1. INTRODUCTION

This policy sets out how NHS North Hampshire Clinical Commissioning Group (herein after referred to as 'CCG') will approach the management of its records. This policy is part of a Records Management Framework that includes additional procedure, guidance, training, audit and strategy. Our records framework fits into the wider context of Information Governance.

All NHS records (including email and electronic documents) are public records under the terms of the Public Records Act 1958 sections 3(1)-(2), and must be kept in accordance with the following statutory and NHS guidelines:

- The Public Records Act 1958 and 1967
- The General Data Protection Regulations 2018
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2016
- The Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- NHS Information Governance: Guidance on Legal and Professional Obligations

Guidance on the management of NHS records is provided by the Department of Health.

The Records Management: NHS code of Practice 2016 sets out a schedule of minimum retention periods for many types of record and is based on legal requirements and professional best practice.

2. SCOPE AND DEFINITIONS

This policy covers all CCG business areas and all information, irrelevant of the media being used to store the information. Corporate records in all formats (paper and electronic), active and inactive, held for use in the organisation, including:

administrative (e.g. corporate, provider services, contracts and commissioning, personnel, estates, finance and accounting, customer services and litigation) including e-mails, other communication tools and text messages

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

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

- **Accountability** – Records are adequate to account fully and transparently for all business actions and decisions, in particular to:
 - protect legal and other rights of staff or those affected by those actions;
 - facilitate audit or examination;
 - provide credible and authoritative evidence.

- **Accessibility** – Records can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist.

- **Interpretation** - The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and were appropriate, how the record is related to other records.

- **Quality** – Records can be trusted - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- **Maintenance through time** - so that the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

- **Security** – Records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

- **Retention and disposal** – Records are retained and disposed of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value. The British Security Industry Association standard (BSIA) EN15713:2009 - Secure Destruction of Confidential Material must be adhered to when destroying confidential information

- **Staff are trained** – so that all staff are made aware of their responsibilities regarding records management.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

3. PROCESSES/REQUIREMENTS

North Hampshire CCG's records are its corporate memory, providing evidence to actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making and protect the interests of the CCG. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The CCG operates within an Information Governance compliance environment. Failure to meet any relevant requirement could result in official sanction, reputation damage and even limits on what data and services we could provide as a business. The CCG must be compliant with the NHS Information Governance Toolkit Data Security and Protection Toolkit (DSPT) and Records Management Code of Practice for Health and Social Care 2016.

The organisational benefits from good records management are:

- control and availability of valuable information assets
- efficient use of staff time
- compliance with legislation and standards
- good utilisation of storage and server space
- a reduction in costs
- support the day to day business that underpins the delivery of a high quality service to our customers
- maintain the integrity of the records
- meet legal requirements
- monitoring and audit cycles

North Hampshire CCG will establish and maintain policies to ensure compliance with the Records Management Code of Practice Health and Social Care 2016.

3.1 Records Management – Components and Principles

The International Organisation for Standardisation (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).

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Records Life Cycle	
Lifecycle Stage	Description
1. Planning	At a corporate level we shall develop and implement policy, procedures and functionality to deliver compliant records management strategy 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. We shall ensure that our records are properly captured into approved filing systems, that they are protected from unauthorised access or change, are assigned the correct data classifications and are named following an agreed standard.
4. Retention	We shall retain non-current and superseded records in our filing system 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.
5. Disposal	Our records shall not be retained indefinitely. At the end of the agreed retention periods, records shall be disposed of and a destruction certificate will be issued. In most cases this will mean controlled destruction; a small percentage of records may become be flagged for permanent retention and will be passed to the appropriate place of deposit (POD).

3.2 General Data Protection Regulations 2018 (GDPR)

Under the General Data Protection Regulations 2018 (GDPR) the definition of ‘data concerning health’ is ‘personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status’ (Article 4(15))

‘Personal Data’ is defined as: ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ (Article 4(1))

Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

There are various GDPR definitions relating to the management of information and records in a health environment. For example, under Article 4;

- **‘processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future;
- **‘filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

For information on categories of data and their assigned definition, please refer to Appendix 3b - Categories of data/information.

3.3 Information Quality

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

- ✓ complete (in terms of having been captured in full)
- ✓ accurate (factually correct, legibly and assured as to the integrity of the record)
- ✓ relevant (the degree to which the data meets current and potential user’s needs)
- ✓ accessible (available when needed)
- ✓ timely (recorded and available as soon after the event as possible) alterations or annotations (must be clearly identifiable, traceable to the author and authorised by an appropriate Senior Manager).

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Clinical records must be timely, accurate, concise and up to date accounts of the assessment and treatment of individual patients. Good clinical record keeping is an integral and vital part of professional practice and may come under scrutiny should any issues arise.

Department/Process managers shall also be clear on what records are required to sufficiently document business activities, and ensure that staff capture them following policy and procedure

3.4 Manual / Paper Records

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

Where it is practical to do so, we shall scan new or legacy paper records following our scanning guidance (this follows standard British Standard (BS) 10008 to protect legal admissibility of scanned paper records). In some cases it might be desirable to hold original ink signed records. This is permissible, although scanning such documents is preferable so long as the scanned version is legally admissible.

Paper copies of records must be kept secure and should be stored in an appropriate locked filing cabinet, office or designated records store on site, or in an approved off-site storage facility, so they are available and accessible to those who need them.

3.5 Records Inventory

We shall use the Information Asset Register's to monitor and understand what collections of records and information we hold and note each documents retention period. We shall work towards organising our records into a Records File Plan that lists our business activities, and the records that they create, in a systematic and organised way.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

3.6 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. It includes a record of what happened so that we can clearly show that we do not have the information any longer.

Disposal of any records shall be *held* if they pertain to an existing / emerging legal matter or request for information – this is known as a Legal Hold. An inventory of the retained records and the reason for the extended period of retention must be maintained.

Our records shall be retained and disposed of following agreed disposal schedules and procedures that are based on the Records Management Code of Practice for Health and Social Care 2016 and business needs. Disposal shall always be carried out following confidentiality and sensitivity requirements. The CCG should not retain records of legacy NHS organisations.

Unilateral disposal of records, particularly if done contrary to disposal schedules or legal holds, is a serious breach of policy.

3.7 Accredited File Shares

Our electronic records shall be saved to our approved and governed file share and shall include sub-folders that assist with disposal management.

Where records contain person identifiable data and special categories of personal data that are considered as personal confidential data or hold commercially confidential information, it is a legal requirement that such data is stored securely. You must ensure such data is stored within the Secure drive and have the correct protective marker applied – please refer to the section 3.9 Security and Access.

As a general rule, original electronic records shall not be saved to ‘offline’ storage such as non-networked computer 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 such as a USB memory stick. This is permissible if the IT Services Acceptable Use Policy is followed, and any new records / versions are saved to the approved storage location as soon as possible and subsequently deleted from the storage device.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

3.8 Naming Electronic Documents

Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the CCG to aid in the management of records.

In constructing a title it is necessary to decide how best to describe the content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title.

Common elements of a title:

- Directorate name
- Date (if applicable)
- Subject
- Document status
- Version number

Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

3.9 Security and Access

Classification of NHS Information - Marking Guidance from NHS England

ALL information the CCG collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works within NHS North Hampshire CCG (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any CCG information or data that they access, irrespective of whether it is marked or not.

Please refer to Appendix 3: Protective Marking Scheme for further information.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

3.10 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.

3.11 Data Backups

All of our data including electronic records are 'backed-up' to offline storage in accordance with the relevant Backup and Business Continuity Policy. It is vital that 'rescued' records are complete copies and are not changed in any way, this includes embedded metadata e.g. date created, data last modified.

Backups are within scope of statutory access to information requests and legal disclosure. Records deleted from user front-end storage, e.g. file shares, shall also be deleted from the back-up and shadow copies. Current back-up policy is that any iteration of electronic data is backed-up for one year before being overwritten / deleted. In short, records that have been deleted from front-end systems within the last year may still be available in the back-up.

3.12 New Technologies – Cloud and Collaboration / Sharing

The use of new technologies to improve working practices, process monitoring and collaboration is becoming increasingly popular. These are characterised by services such as cloud storage and collaboration spaces being held outside of traditional on-site technology infrastructure.

The requirements of this policy shall apply to such technology because they are handling our information and records. Assurances must be in place to ensure that data retention schedules are met and data is fully deleted, to include, back-up copies and 'other' structures that may refer to or directly reference the data, for example, a document index.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

3.13 Email Records / Electronic Communication

Email is a key communication tool. 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.

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

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

Staff shall regularly housekeep their Mailboxes so that transitory and spam type emails are disposed of. Managers shall ensure all required email records are transferred from a staff leaver's Mailbox to the approved store. Other forms of electronic communication such as Instant Messaging, voice recording and video conferencing will likely become more commonplace. These 'recordings', if retained, shall be managed under this policy.

3.14 Long Term Access and Protection – Record Preservation

The CCG will take steps to ensure that records remain accessible and are not damaged during their retention; for some records this could be many decades. Such lengths of time require preservation management.

Our records shall be protected from unauthorised access and natural risks such as flooding and fire. A risk assessment of all storage solutions (on or off-site) must be undertaken to ensure the area meets the required structural and environmental standards, for example, IGTK standard – 14-301. Electronic records are at a particular risk of digital obsolescence and degradation of media. We shall undertake precautions to ensure the long term accessibility of electronic content including: using ubiquitous and open formats e.g. PDF, DOCx; regular refreshing and error-checking of storage media; maintaining all records on networked and backed-up drives rather than removable media storage e.g. CDs, USBs; and assessing the digital preservation risks of any new system.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

4. ROLES AND RESPONSIBILITIES

Position or group	Description of Records Management Responsibility
Accountable Officer	Accountable for the proper and compliant conduct of records management across the organisation.
Caldicott Guardian	The Caldicott Guardian is Responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. They will support work to enable information sharing where it is appropriate to share, and advice on possible choices for meeting compliance when processing information.
Data Protection Officer	The Data Protection Officer (DPO) has the responsibilities as set out in the GDPR guidance and is responsible to feedback any Information Governance issues to the CCG Finance and Assurance Committee. The DPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident. They will also be part of the Data Protection Impact Assessment process on behalf of the CCG.
Senior Information Risk Owner (SIRO)	Take ownership of the organisation's information risk policy. Acts as advocate for information risk on the board. Drive culture change with regard to information risks in a realistic and effective manner. Is advised and supported by the Information Governance Manager.
Records Manager	Day-to-day operational management of the records management programme and framework. Drafting policy and procedures. Conducting audits. Supporting and training staff. Providing records management services to customers.
Information Asset Owners (IAO)	The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role.
Data Custodians (DC's)	Data Custodians are required to support the IAO's and SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. The Information Governance Team will provide local face to face IG training if required and will monitor staff compliance by way of the e-LfH platform.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

All staff	All staff, and those working on behalf of the organisation, are expected to follow this policy and its procedures. All staff who create and use records as part of the delivery of CCG business. This covers records in all formats (paper and electronic), both active and inactive.
------------------	---

5. TRAINING

All staff are required to comply with the CCG IG Staff Handbook which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. Information Governance is a framework drawing these requirements together; therefore it is important that staff receive the appropriate training.

The CCG will ensure all staff receive annual Information Governance training appropriate to their role through the online E-Learning for Health training tool or face to face training (if offered). Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the annual Information Governance Training.

On joining the organisation, CCG staff will receive a copy of the Information Governance staff handbook and will be required to sign and return a receipt to the SCW IG Team.

6. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

Both new policies, and existing policies when reviewed, come within the Public Sector Equality Duty. This means that policy authors must consider whether the policy will be effective for all patients and/ or staff. This process is called equality impact assessment.

This policy has been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.

7. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be monitored by the Finance & Performance Committee to ensure any legislative changes that occur before the review date are incorporated.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Our performance in records management compliance shall be audited following a scheduled plan using a defined audit methodology. Information Asset Owners will have direct responsibility for ensuring their information practices are audited with support from the Records Manager and Information Governance team. Where non-compliance or improvements could be made then these shall be agreed with process owners / managers and subsequently followed up.

This policy, along with its supporting procedures, shall be reviewed no later than two years after approval or earlier should there be significant changes to the regulatory environment or organisation.

Failure to comply with this policy may result in ineffective working and an inability to meet the requirements of the Freedom of Information and the General Data Protection Regulations 2018. Where the policy is breached, this must be reported via the CCGs incident reporting process and the Data Protection Officer and Caldicott Guardian informed, if required.

8. REVIEW

In compliance with Data Security and Protection Toolkit requirements, this policy will be reviewed annually. The policy review will take into account comments received from the Finance and Performance Committee and will be reviewed by the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer and Head of Information Governance.

9. REFERENCES AND ASSOCIATED DOCUMENTS

- Information Commissioners Office (Data Protection Act 2018 and General Data Protection Regulation) – www.ico.gov.uk/
- National Archives (Public Records) – www.nationalarchives.gov.uk
- Data Security and Protection Toolkit – <https://www.dsptoolkit.nhs.uk>
- NHS England (Document and Records Management Policy Final V3) - <https://www.england.nhs.uk/>
- Records Management Code of Practice for Health and Social Care 2016 - <http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf>

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

- Government Security Classifications April 2014 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
- NHS North Hampshire CCG Information Governance Policy
- NHS North Hampshire CCG Information Governance Management and Strategy Framework
- NHS North Hampshire CCG Information Governance Handbook
- NHS North Hampshire CCG Information Governance Confidentiality and Safe Haven Policy
- SCW CSU IT Services – Backup and Business Continuity Policy
- SCW CSU IT Services – Equipment Disposal Policy

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Appendix 1: Key Records Management 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.
General Data Protection Regulations 2018	<p>Regulates the processing of personal data relating to living persons. Article 5 of the GDPR requires that personal data shall be:</p> <ul style="list-style-type: none"> a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

	<p>statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and</p> <p>f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”</p>
Data Protection Act 2018 (DPA 2018)	The Data Protection Act 2018 replaces the Data Protection Act 1998 and legislates to an equivalent to the GDPR but includes national derogations not covered by the GDPR. The DPA 2018 should be read in conjunction with the GDPR.
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.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Appendix 2: Clinical Records Guidance

GDPR Recital number 35 clarifies that Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes:

- information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person;
- a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;
- and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Good clinical record keeping is an integral and vital part of professional practice which contributes to a high standard of:

- The delivery of clinical care
- Continuity of care
- The sharing of information and improving communication between parties
- Business and reporting purposes

Clinical records must be timely, accurate, concise and up to date account of the assessment and treatment of individual patients.

Some CCG business activities will create or receive clinical records. Information held in these records will relate to any aspect of patient health, treatment and other care they receive and, by their nature, are considered as OFFICIAL-SENSITIVE: PERSONAL.

Only business areas that specifically require clinical records to carry out their work should have access to them. If you receive clinical records and you are not sure why then report this to your Manager and (relevant IG contact in

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

The Team or individual employees are responsible for the safeguarding of confidential information held as paper records (in a structured filing system) and electronically (on computers and within an agreed filing procedure). Please ensure there are robust 'track and trace' mechanisms place for all paper records, e.g. tracer cards and access to electronic information must be appropriately restricted.

Unavailable, mislaid or lost clinical records are a serious risk and immediate action must be taken. The appropriate Department must log this as an incident on DATIX and carry out an investigation

Any unauthorised use of clinical information, e.g. searching for information about a relative or any use of information outside of a "legitimate professional relationship" may lead to immediate disciplinary action. This would be viewed as a breach of confidentiality.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Appendix 3a: Protective Marking Scheme

Classification of NHS Information - Marking Guidance from NHS England

The new Government Security Classifications levels are;

OFFICIAL

Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. The CCG will operate exclusively at this level including the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

SECRET

Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET

Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

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

This simplified procedure will make it easier and more efficient for information to be handled and protected. The new procedure places greater emphasis on individuals taking personal responsibility for data they handle.

All information used by the CCG is by definition 'OFFICIAL.' It is highly unlikely the CCG will work with 'SECRET' or 'TOP SECRET' information.

Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.
2. A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but should have additional measures applied in the form of OFFICIAL-SENSITIVE.
3. This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic records.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

4. In addition to the marking of OFFICIAL-SENSITIVE further detail is required due to the content of the document or record, i.e.:

OFFICIAL – SENSITIVE: COMMERCIAL

Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed.

Or

OFFICIAL – SENSITIVE: PERSONAL

Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Such documents/records should be marked with the caveat ‘OFFICIAL-SENSITIVE: COMMERCIAL or SENSITIVE’ in capitals at the **top and bottom** of the page.

In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

NHS Confidential

In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

How to handle and store OFFICIAL information;

EVERYONE is responsible to handle OFFICIAL information with care by:

- Applying clear desk policy
- information sharing with the right people
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

How to handle and store OFFICIAL – SENSITIVE information;

All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, OFFICIAL-SENSITIVE:PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

- Always apply appropriate protection and comply with the handling rules
- Always question whether your information may need stronger protection
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains, etc
- Only print sensitive information when absolutely necessary
- Send sensitive information by the secure email route or use encrypted data transfers
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control
- Store information securely when not in use and use a locked cabinet/drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details
- Only in exceptional cases, where a business need is identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact the Corporate IG team for further advice
- The use of pin code for secure printing is both widely available and preferable way to manage the printing process

There is no need to apply the new classification procedure retrospectively.

Our Accredited File Shares shall include protected folders and permission protocols where OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIVE: PERSONAL information is held. Access to OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIVE: PERSONAL paper files should be restricted and monitored thus ensuring adequate security measures are in place. NB: All paper records must be tracked to ensure their exact location is known at all times.

Access restrictions to records shall be proportionate. Wherever possible, records and information should be available to all staff to aid information sharing, and reduce duplication and data volumes. Although clinical records must be kept secure on a need-to-know basis, this does not mean that they cannot be made available in a timely fashion to those who justifiably need access.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Example descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL and respective category of data/information as detailed in Appendix 3b.

Category /data type	Definition	Marking
Appointments (Commercially confidential information)	Concerning actual or potential appointments not yet announced	OFFICIAL-SENSITIVE: COMMERCIAL
Barred (Personal Confidential Data)	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
Board (Commercially Confidential Data)	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 (Commercially Confidential Information)	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts (Commercially Confidential Information)	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL-SENSITIVE: COMMERCIAL
For Publication (Commercially Confidential Information)	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(Commercially Confidential Information)	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

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Patient Information (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning identifiable information about patients	OFFICIAL-SENSITIVE: PERSONAL
Personal (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning matters personal to the sender and/or recipient	OFFICIAL-SENSITIVE: PERSONAL
Policy (Commercially Confidential Information)	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 (Commercially Confidential Information)	Corporate information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning identifiable information about staff to include investigations, disciplinary hearings and grievances.	OFFICIAL-SENSITIVE: PERSONAL

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019

Appendix 3b - Categories of data/information.

Please note that the categories of data/information listed below, will be used or referred to in all CCG Policies. The purpose of this approach is to ensure a consistent approach is adopted.	
Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: The racial or ethnic origin of the data subject Their political opinions Their religious beliefs or other beliefs of a similar nature Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 Genetic data Biometric data for the purpose of uniquely identifying a natural person Their physical or mental health or condition Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

Version Number: 4	Issue/approval date: 25 th June 2018
Status: Final	Next review date: April 2019