NHS
Hampshire, Southampton and
Isle of Wight
Clinical Commissioning Group

RECORDS MANAGEMENT POLICY

Document number	IG/010/V1.2
Version	Version 1.2
Approved by	Policy Sub Group
Document author	Information Governance Consultant, South Central & West Commissioning Support Unit
Executive lead	Chief Finance Officer (Senior Information Risk Owner)
Date of approval	18 October 2021
Next due for review	April 2022

National Inquiry into the COVID-19 Pandemic Response

The Prime Minister has announced that the Government will hold an independent public inquiry in relation to the Government and public sector response to the COVID-19 pandemic.   The purpose of a statutory inquiry is to ensure transparency and lessons are learned. As such they have considerable evidence gathering powers. It is not clear at this stage the scope of the Inquiry and how individual organisations will be involved. However, in the circumstances all staff within Hampshire Southampton and Isle of Wight CCG are now instructed to **retain** all documents; correspondence; notes; emails; and all other information, however held, which contain or may contain content pertaining directly or indirectly to the CCG response to the COVID-19 pandemic and key decisions made as part of the recovery.

Hampshire, Southampton and Isle of Wight CCG is committed to fully cooperating with any inquiry openly and transparently. In due course, once the terms of reference of the inquiry have been confirmed the CCG may be required to disclose relevant documents to the inquiry. We will need to be clear how and why key decisions were taken. Access to relevant documents will be essential to enable those who are required to give evidence to articulate what happened during a period when many issues were being addressed at great pace. Any loss of documentation will hamper the investigation, cause delay and increase costs and could harm the reputation of the NHS.

Should you have any questions, please contact Tracy Davies - tracy.davies4@nhs.net or Jackie Zabiela - jzabiela@nhs.net who are part of the Public Inquiry Working Group.

Version control sheet

Version	Date	Author	Comment
V1.1	04/02/21	Jackie Thomas, Senior IG Consultant, SCW CSU	Review and update in line with planned merger of HIOW Partnership of CCGs, West Hampshire CCG and Southampton CCG to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021
V1.2	03/10/21	Jackie Thomas, Senior IG Consultant, SCWCSU Governance Manager, CCG	Amendments following review by CCG Governance Leads and re-format into CCG approved template.

EQUALITY STATEMENT

Equality, diversity and human rights are central to the work of the Hampshire, Southampton and Isle of Wight (HSI) CCG. This means ensuring local people have access to timely and high quality care that is provided in an environment which is free from unlawful discrimination. It also means that the CCG will tackle health inequalities and ensure there are no barriers to health and wellbeing.

To deliver this work CCG staff are encouraged to understand equality, diversity and human rights issues so they feel able to challenge prejudice and ensure equality is incorporated into their own work areas. CCG staff also have a right to work in an environment which is free from unlawful discrimination and a range of policies are in place to protect them from discrimination.

The CCGs' equality, diversity and human rights work is underpinned by the following:

- NHS Constitution 2015.
- Equality Act 2010 and the requirements of the Public Sector Equality Duty of the Equality Act 2010.
- Human Rights Act 1998.
- Health and Social Care Act 2012 duties placed on CCGs to reduce health inequalities, promote patient involvement and involve and consult the public.

Contents

Equality Statement 4

1. Introduction 6
2. Scope and definitions 8
3. Processes / requirements 9
4. Roles and responsibilities 19
5. Equality Act 2010 – Equality analysis 20
6. Training 20
7. Dissemination 21
8. Monitoring compliance and effectiveness 21
9. Review 22
10. Stakeholder / consultation information 22
11. References and associated documents 22

Appendix A Clinical Records Guidance 24

Appendix B Electronic Records Management 26

Appendix C Scanning Records Guidelines and Procedure 28

Appendix D Protective Marking Scheme 33

Appendix E Glossary of Terms 39

Appendix F Example Record Disposal Request Certificate 42

Appendix G Equality Impact Analysis 43

1. Introduction

This policy sets out how NHS Hampshire, Southampton & Isle of Wight Clinical Commissioning Group (hereinafter referred to as the CCG) will approach the management of its records. This policy is part of a Records Management Framework that includes additional procedures, guidance, training, audit and strategy. Our records framework fits into the wider context of Information Governance. A records management policy embeds the effective management of records in an organisation. It will ensure the CCG keeps the records we need for business, regulatory, legal and accountability purposes.

All NHS records (including email, electronic documents and audio and visual) 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 UK General Data Protection Regulations 2016 (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Access to Health Records 1990
- Health & Social Care Act 2008
- Regulation of Investigatory Powers Act 2000
- Criminal Procedure and Investigations Act 1996
- Records Management Code of Practice 2021
- The Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- NHS Information Governance: Guidance on Legal and Professional Obligations.

a. The Public Records Act 1958 is an Act of Parliament to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.

b. The UK GDPR regulates the processing of personal data. It is implemented in the UK by the Data Protection Act 2018 (DPA) which complements the UK GDPR. The two pieces of legislation must be read together.

c. The Data Protection Act 2018 is an Act of Parliament which regulates the processing of personal data relating to living individuals, including the obtaining, holding, use or disclosure of such information. Access to the health records of living patients is governed by this Act.

d. The Freedom of Information Act 2000 is an Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor’s Code of Practice on the management of records is issued under section 46 of this Act.

e. The Access to Health Records Act 1990 is an Act of Parliament that regulates access to the health records of a deceased person.

f. The Health and Social Care Act 2008 regulation 17 requires health and care providers to maintain detailed, accurate and complete records.

g. The Regulation of Investigatory Powers Act 2000 which permit the 'interception' of communications. Such interception must be proportionate to the needs of the organisation, society and the users of the communication system.

h. Criminal Procedure and Investigations Act 1996 sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation, and related matters.

i. The Records Management Code of Practice 2021 was published by NHSX on 5 August 2021. It is a best practice guide for the management of records for those who work within or under contract to NHS organisations in England. They are based on legal requirements and professional best practice.

j. The Common Law Duty of Confidentiality is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases. If information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent.

k. Confidentiality: NHS Code of Practice sets out what health and care organisations have to do to meet their responsibilities around confidentiality and patients' consent to use their health records. It's based on legal requirements and best practice.

l. NHS Information Governance: Guidance on Legal and Professional Obligations provides guidance on the range of legal and professional obligations that affect the management, use and disclosure of information.

2. Scope and definitions

The CCG directorates fall within the scope of this document. This includes staff who are employed on a permanent or fixed term basis, contractors, temporary staff and secondees.

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, electronic and audio and visual), 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.
- service user / clinical related (e.g. complaints, safeguarding, Continuing Healthcare records).

Clinical environments should operate in accordance with appropriate and necessary safe haven principles. To include all services that require personal confidential data to flow between internal and external stakeholders (refer to Appendix A).

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:

- **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.

3. Processes / requirements

The CCG and, where applicable, its legacy organisations 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 Data Security and Protection Toolkit (DSPT) and Records Management Code of Practice 2021.

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
- Maintain the integrity of the records
- Meet legal requirements
- Monitoring and audit cycles.

The CCG will establish and maintain policies to ensure compliance with the Records Management Code of Practice 2021.

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 2021).

Records Life Cycle	
Lifecycle Stage	**Description**
1. Creation & receipt	This is where a record is created, it is known as the first phase. Records can be created by an internal source or received from an external source. We shall ensure that our records are properly captured into an 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.
2. Use	This is when records are used on a day to day basis to help generate organisational decisions, document further actions or support other CCG improvement operations.
3.Maintenance	Maintenance is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision.
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, for paper records in off-site storage or confidential waste bin destruction, a destruction certificate will be issued. In most cases this will mean controlled destruction; a small percentage of records may have historical value and will be sent to a Place of Deposit (POD) where they will be kept for the future of the organisation and may never be destroyed. This is final phase of a records lifecycle (please refer to the Records Management Code of Practice 2021 for guidance as to which records could have historic value). If you are unsure whether your records have historical value, please get in touch with the Data Protection Officer.

Declaring a Record

Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' (refer to the Records Management Code of Practice for guidance). This process is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.

A record is declared at the point that a final version is created. That is the contents of the record are frozen at this and should remain un-editable from thereon. Some activity will be predefined as a record that needs to be kept, such as clinical records.

It is important that the principles of provenance are also considered. For example, that the properties as stated in the original remains as it was at the time the record was created.

Care should be taken to consider the entirety of the record at the point of declaration. For example, ensuring that external information on which that record is reliant (such as a page on the intranet) is also captured.

Data 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).

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 (refer to Appendix A for guidance).

Alterations or annotations, particularly in relation to clinical records (e.g. continuing healthcare, safeguarding), must be clearly identifiable, traceable to the author and authorised by an appropriate Senior Manager.

Manual / Paper Records

All staff are encouraged to save in electronic format wherever applicable. Records which need to remain in paper format are often 'Sealed' contract records which are usually identified by an embossed stamp and are executive level, or clinical / service user records e.g. Complaints, Continuing Healthcare, Safeguarding. For records which you feel cannot be digitised and require off site storing please get in touch with the teams Data Custodian.

The movement and location of paper records should be controlled and tracked to ensure that a record can be easily retrieved at any time. This will enable the original record to be traced and located if required and must be held in a shared location.

Paper file storage, on and off-site must be secured from unauthorised access and meet fire regulations.

Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of the CCG.

Where it is practical to do so, we shall scan new or legacy paper records following our scanning guidance (see Appendix C); 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.

Records Inventory

We shall use the Information Asset Registers to monitor and understand what collections of records and information we hold and note each documents retention period.

Long Term Access and Protection – Record Preservation

We shall take steps to ensure that our 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 and off-site) must be undertaken to ensure the area meets the required structural and environmental standards. 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.

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 the shared network drive. Please refer to Appendix B for further guidance on managing electronic records.

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.

A Legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation or inquiry. Organisations have a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated. Staff must immediately notify the Data Protection Officer if they have been notified of a Litigation, Investigation or Inquiry or have reasonable foresight of a future Litigation, Investigation or Inquiry as this could result in records being held beyond their identified retention period.

The Prime Minister has announced that the Government will hold an independent public inquiry in relation to the Government and public sector response to the COVID-19 pandemic. The purpose of a statutory inquiry is to ensure transparency and lessons are learned. As such they have considerable evidence gathering powers. It is not clear at this stage the scope of the Inquiry and how individual organisations will be involved. However, in the circumstances all staff within Hampshire Southampton and Isle of Wight CCG are now instructed to ***retain*** *all documents; correspondence; notes; emails; and all other information, however held, which contain or may contain content pertaining directly or indirectly to the CCG response to the COVID-19 pandemic and key decisions made as part of the recovery.*

Our records shall be retained and disposed of following agreed disposal schedules and procedures that are based on the Records Management Code of Practice 2021 and business needs. Disposal shall always be carried out following confidentiality and sensitivity requirements.

If a declared record is deleted and/or destroyed once its retention period has been reached, then a Records Disposal Certificate, Electronic Metadata destruction stub or email confirmation from the IT Services confirming that the electronic records have been deleted must be completed and saved in order to prove that the record existed, met its retention and was disposed of. See Appendix F for an example copy of a Record's Disposal Certificate.

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

Protective Marking Scheme Security and Access

Classification of NHS Information - Marking Guidance from NHS England and NHS Improvement

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 the 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 as CONFIDENTIAL or not.

The CCG is working to existing IG guidance and where necessary marking documents as either CONFIDENTIAL or COMMERCIALLY SENSITIVE.

NHS England and other NHS / public bodies have adopted the Government Security Classifications, published April 2014. Whilst the CCG has not yet adopted this, any information received from an NHS organisation marked as OFFICIAL-SENSITIVE (PERSONAL or COMMERCIAL) should be treated as Confidential. Please refer to Appendix D for further information.

The CCG will work towards implementation of the Government Security Classifications over 2021/22.

Line of business systems / databases

Many of our and 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 along with the Data Protection Impact Assessment Framework when implementing, procuring or using databases or setting up file shares (including Cloud platforms).

Electronic records that are uploaded to databases should be deleted from local systems, e.g. Inbox. It is bad practice to duplicate information across systems.

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. Mechanisms must be in place to ensure that data retention schedules are met and data is fully deleted, to include, backup copies and ‘other’ structures that may refer to or directly reference the data, for example, a document index. Original copies of any documentation shared on cloud storage / collaboration spaces must be retained on network drives in accordance with the CCGs records management procedures.

Data Backups

All of our data including electronic records are ‘backed-up’ to offline storage in accordance with the IT Backup 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. The IT Backup Policy provides detail on the expected level of backup and recovery of key technology solutions. In short, records that have been deleted from front-end systems within the last year may still be available in the back-up.

Records Security: Work Base, Home Working, Agile Working

Only remote access solutions that are provided or agreed with the CCG can be used to access our networks when away from CCG workplaces.

All person identifiable data or commercially sensitive data must be stored within a secure drive and have the correct protective marker (security classification) applied. CCG staff should contact IT support to request a secure folder.

All staff are responsible for ensuring that any data or assets taken home, data printed off at home or handwritten notes / minutes of meetings are kept secure and confidential and stored in a locked cupboard (not accessible to family members) until either able to take to the office for confidential shredding or destroyed by shredding, combustion or pulping. Domestic waste that could lead to Personal Confidential Data remaining accessible should not be used.

Users are also responsible for information that is displayed on screens.

Staff must not use home email accounts or private computers to hold or store any sensitive records or information which relates to CCG business activities.

Removable Media must be owned and encrypted by IT Services. Ideally, personal data should not be stored on any removable media, however if there is no other option ensure this data is stored on a corporate encrypted device and deleted once transferred to identified secure area folder.

When printing paper records, especially sensitive documents, ensure appropriate measures have been taken.

Never leave your computer screen open when unattended. Always lock it using the keys Control + Alt + Delete and then click on ‘Lock This Computer

Missing and Lost Records

A ‘missing record’ is when a record cannot be found, or is not available when required.

In the event of a missing record, a thorough search must be undertaken. This will include initiating a search at the base (this may include facilitating/requesting searches at non-CCG locations if appropriate, e.g. GP surgeries or shared office buildings, in addition to reviewing the tracking history of the record.

If after 5 working days, the record has not been found, the missing record must be reported to your line manager and Information Asset Owner / Data Custodian, as well as the SCW CSU Information Governance Team and logged on Datix in accordance with the CCG IG Incident Management and Reporting Procedure. The severity of the incident will determine the level of investigation required.

The missing record should be marked as missing in any electronic / manual tracking systems in use, and the record must be reconstituted, populated as far as possible with all the relevant information and clearly marked as a 'reconstituted record'. If applicable, the electronic / manual tracking system must be updated to note that the record has been reconstituted and on what date this occurred.

When the original record is located the temporary and original set of records should be merged together. If applicable, the electronic / manual tracking system must be updated to state that the original records were located and merged with the reconstituted record, and with the location of the merged records. Update Datix / inform the SCW CSU IG Team. If after 6 months, the record is still missing, it is reasonable to assume that the original set of records has been lost. Inform the SCW CSU IG Team.

4. Roles and responsibilities

Position or group	Description of Records Management Responsibility
Managing Director TBC	Accountable for the proper and compliant conduct of records management across the organisation.
Caldicott Guardian and Executive Team	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. The Executive Team cascade requirements of the policy to respective departments and support its implementation.
Data Protection Officer	The Data Protection Officer (DPO) has the responsibility to feedback any Information Governance issues to the Executive Management Team. 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 Steering Group (TBC).
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.

Position or group	Description of Records Management Responsibility
Data Custodians (DC's)	Data Custodians are required to support the IAO's and the 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 consult OD portal and link to the e-LfH platform.
Department / Process managers	Ensure records produced by their respective activities are identified and captured following policy. Ensure that staff have attended required record keeping training. Work with local IG and records roles.
All staff	All staff, and those working on behalf of the organisation, are expected to follow this policy and its procedures. All staff are responsible for keeping a record of any significant business transaction conducted as part of their duties for the organisation.. The record should be saved appropriately, a retention period assigned and access controls applied if necessary.

5. Equality Act 2010 – Equality analysis

An Equality Impact Analysis (EIA) has been completed as this policy was assessed as having a medium impact on individuals with characteristics protected under the Equality Act. There is a risk of negative impact if this and related policies are not followed; note particular requirements under Section 22 of the Gender Recognition Act 2004. A copy of the EIA is attached at Appendix G.

6. Training

All staff are required to comply with the 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 delivered by the Information Governance Team. 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, staff will receive a copy of the Information Governance Staff Handbook and will be required to confirm they have read and understood their responsibilities.

7. Dissemination

This policy will be made available to staff on the IG page of the CCG website, with a link to the appropriate page also available on the staff intranet / StayConnected portal.

8. Monitoring compliance and effectiveness

This policy will be monitored by the Policy Sub Group*,* to ensure any legislative changes that occur before the review date are incorporated.

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

Failure to comply with this policy may result in ineffective working and an inability to meet the requirements set out in relevant legislation. Where the policy is breached, this must be reported via the local incident reporting process and the Data Protection Officer and Caldicott Guardian informed, if required.

9. Review

This policy will be reviewed annually by the SCW CSU IG Team, or earlier if required by law.

10. Stakeholder / consultation information

This policy was already in place in the HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG prior to the merger to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021.

It has been through an internal process and reviewed by the IG Team, South Central & West Commissioning Support Unit, with input from the IG Transition Group, DPO, Governance Managers and reviewed by the SIRO.

11. References and associated documents

Title	**Website / intranet address**
Information Commissioners Office (Data Protection Act 2018 and UK 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
Records Management Code of Practice 2021	Records Management Code of Practice - NHSX
Government Security Classifications	Government Security Classifications - GOV.UK (www.gov.uk)
CCG Information Governance Policy	Information Governance (hampshiresouthamptonandisleofwightccg.nhs.uk)
CCG Staff Handbook – Information Governance	Information Governance (hampshiresouthamptonandisleofwightccg.nhs.uk)

Title	**Website / intranet address**
CCG Individual Rights Policy	Information Governance (hampshiresouthamptonandisleofwightccg.nhs.uk)
CCG Information Security Policy	Policies - StayConnected (hampshiresouthamptonandisleofwightccg.nhs.uk)
CCG IT Backup Policy	
CCG IT Disposal Policy	
CCG Remote Working & Portable Devices Policy	
CCG Acceptable Use Policy	

Appendix A Clinical Records Guidance

UK 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 CONFIDENTIAL (or 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 the IG team.

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 (refer to the Information Incident Management and Reporting Procedure) 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.

Appendix B Electronic Records Management

Electronic Filing Structure

Electronic records management needs to be very carefully considered and structured to ensure the integrity of the records is not compromised upon capture and they remain retrievable for as long as they are required.

The filing structure reflects the relationship of business activities through careful structuring of folders (with meaningful titles) ‘containing’ the records. This structure illustrates what the organisation’s business. Therefore, organised filing structures support records management by providing an understandable, accessible and secure location for all records which encourage users to work within it. This helps an organisation reduce the risk of business critical information being lost within an uncontrolled file system. It also helps motivate users to move records out of personal drives or emails accounts.

It is important to use clear, logical and descriptive titles for folders. Aim to make the name of the folder descriptive of its content or purpose and avoid the use of any ambiguous terms such as ‘general notes’ or ‘miscellaneous information’.

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.

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 Remote Working & Portable Devices 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.

Naming Convention

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 document or record title:
- Date format YYYMMDD
- Subject /Description – clear, succinct and descriptive
- Document status - FINAL, REVIEW or DRAFT
- Version number - who numbers to denote final versions and decimal numbers to denote under review or draft versions.

Windows and Office 365 restrict file paths to 255 characters. Therefore, the use of acronyms may be need to be used on this occasion. Do not use obscure abbreviations of acronyms as they can become obsolete and may have more than one meaning. Best practice is to retain a glossary of acronyms. Please contact the IG Team for advice and guidance.

Electronic Communication

Email and other methods of electronic communication are designed as a communication tools and not as 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.
- Remember to change the title of the email to accurately reflect the content.
- Consider if all attachments and embedded documents also need to be saved to preserve the context.

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 patient record.

Appendix C Scanning Records Guidelines and Procedure

Introduction

The campaign for a paperless or paper-light organisations is promoted in order to meet Government targets, reduce duplicate records, improve information sharing, reduce cost and save space. Staff may consider the option of scanning paper records in to electronic format. Electronic scanned documents are easier to locate and can be made available to a larger audience than paper copies.

The aim of these guidelines is to raise awareness, disseminate good practice and create uniformity across the CCG. They adopt the Records Management Code of Practice 2021 which provides specific guidelines on health, social care and corporate records.

Records Management Code of Practice 2021
Scanned Records

Where scanning is used, the main consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an ***authentic record*** *and there are technical and organisational means to ensure the scanned records maintain their* ***integrity, authenticity and usability as records****, for the duration of the relevant retention period.*

The standard 'BS 10008 Electronic Information Management – Ensuring the authenticity and integrity of electronic information' specifies the method of ensuring that electronic information remains authentic.

If this is a record type which must or may be selected and transferred to a place of deposit (refer to Records Management Code of Practice for Health and Social Care 2016, Appendix 3*), the place of deposit should be asked whether they wish to preserve that hard copy and/or the scans. If the hard copy is retained, this will constitute 'best available evidence' for legal purposes, rather than the scanned copy.*

Procedure for scanning paper records

Staff need to ensure electronic records and information carry evidential weight and legal admissibility in a court of law. **Legal admissibility** concerns whether or not a piece of evidence would be accepted by a court of law and compliance with this standard is achieved through the implementation of the recommendations in BS1008 Electronic Information Standard. This Standard provides guidance to ensure, as far as possible, that electronic documents will be accepted as evidence by the courts.

The contents of the standard include, the availability and accessibility of the information, the use of document management, the management of quality issues related to document scanning processes, the provision of a full audit trail for the life of a piece of electronic information, copyright and system maintenance. The key is to ensure that the process under which documents are managed is as important as the technology used- where a document is reproduced, it should accurately reproduce the contents of the 'original' document.

By virtue of the Freedom of Information Act 2000, NHS England is required to conform to the 'BS1008 Electronic Information Standard.'

<u>Preparation of records for scanning</u>:

- An assessment of the robustness of documents to be digitised is required. Quality of paper and age will be a consideration.
- Has the record and/or document reached it’s review or destruction date? Check the retention schedule before you scan.
- Photographs – please proceed with caution, check the quality of the scanned copy and consider retaining the original photo if the integrity of the image has been compromised.
- Before scanning, all staples, plastic wallets and other binding devices must be removed from documents. There may also be post-it notes, odd-sized drawings or items that are not to be scanned (e.g. brochures, duplicate copies of documents). Remove finger prints and dust from the scanner glass.
- Protect the integrity of the record – were possible do not remove blank sheets as this could suggest that the scanned copy has been altered.
- Where documents in paper form are photocopies and the photocopies are to be scanned, the photocopied parts of the document should be identified and recorded as being from photocopies.
- Documents and records used by the CCG can potentially be required in support of litigation and submitted as evidence as part of legal or tribunal proceedings.

- Signed paper copies – does the original document with wet signature need to be retained for legal purposes?

  - The Law Society provides guidance on electronic signatures and scanning documents. Please click on following link for further information - https://www.lawsociety.org.uk/support-services/advice/practice-notes/execution-of-a-document-using-an-electronic-signature/

  - 2017/2018 NHS Standard Contract extract –

    Section 15: Signature of contracts and variations.

    Where a group of commissioners wishes to enter in to a contract with a provider, each of the commissioners must sign the contract and cannot delegate this responsibility to another commissioning body.

    Contracts must be signed physically, in hard copy form, by each party. As set out in GC38, this can be done in counterpart form where necessary. Such hard copy signatures can be physically returned to the co-ordinating commissioner by post, but can alternatively be scanned and returned to the co-ordinating commissioner by email. The co-ordinating commissioner should maintain a record of all contract signatures and should provide copies to other commissioners for audit purposes.

    Each party must ensure that the contract is signed by an officer with the appropriate delegated authority. The use of cut-and-paste electronic signatures, applied by more junior staff on behalf of authorised signatories, is not permitted.

    We recognise that the collection of signatures from commissioners is a time-consuming process. Variations may therefore be signed by the provider and the co-ordinating commissioner (on behalf of all commissioners) only, rather than by all commissioners (see GC13.3). Commissioners must therefore ensure that their collaborative agreements set out very clear arrangements through which Variations are agreed amongst commissioners, prior to signature by the co-ordinating commissioner. The co-ordinating commissioner must maintain a record of evidence that each variation has been properly approved by all commissioners (whether or not they are directly affected by the variation –

because all are parties to the contract being varied) and must be prepared to confirm to the provider that it has the agreement of all commissioners, before a variation is signed.

The NHS England Standard Contract Team's view (email dated 28 September 2017) *is that a hard copy should always be retained, for the contract period and an appropriate period following the expiry or termination of the contract. However, this is a local decision and parties to the contract may choose to scan in copies of their contracts, rather than retain hard copies. Commissioners may, therefore, choose to run a dual system of retaining hard copies and electronic copies for a period, and quality assure the scanned version.*

Scanning process:

- All pages need to be straight and the correct direction for readability when viewing.
- The correct page size needs to be used so items are not cut off and/or space is not wasted around the document.
- Clarity of the document is also important – scanning resolution should be not more than 300 dots per inch or 118 dots per centimetre. Everything on the original document must be able to be read once scanned into the computer. The contrast and darkness may need to be adjusted to pick everything up.
- Pages with front and backs need to have both scanned in. Check to see if the scanner has a duplex feature.
- Always double check your scanner settings so that you are NOT scanning images to a high resolution that will create huge image files.
- **Do not** use the scanner's default naming standard. Remember to use a meaningful naming convention, i.e. the name reflects what the document is, the version (if applicable) and the date.
- Ensure scan is saved to a safe and secure specified location, for example, accredited file share on a secure network. NB: in the event of the scanning process creating a temporary copy on a PC desktop or mailbox, remember to fully delete these copies.
- Information should be stored and maintained in a file format that cannot be edited such as Portable Document Format (PDF) or Tag Image File Format (TIFF).

- Quality control procedures should be established to check for missing images. Does the original document contain amendments that cannot be identified on the scanned image and check the quality of the scanned image – is it readable, not skewed and not blurry or grainy. If in doubt, retain the original document or record and reference that a scanned copy exists.

It is important to be able to demonstrate to a court that your quality controls are adequate.

Please do not shred originals until you are sure that the scanning and indexing processes have been completed properly and the data has been backed-up.

Appendix D 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.
4. In additional 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: COMMERICAL 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.

<u>NHS Confidential</u>
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.

- 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
- 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 if identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties.
- 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.

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

Category /data type	Definition	Marking
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
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	Concerning identifiable information about staff to include investigations,	OFFICIAL-SENSITIVE: PERSONAL

Category /data type	Definition	Marking
Categories' of Personal Data)	disciplinary hearings and grievances.	

Appendix E: Glossary of Terms

Term of Abbreviations	What it stands for
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Declaration	Declaring a document as a record is a formal point of transition when it passes into corporate ownership, i.e. corporate record. Once a document is declared as a record, it must be protected from change and assigned a retention period. When this retention period expires, the record must be appraised for deletion. For advice on retention, contact the information governance department.
Electronic Document	Information recorded in a manner that requires a computer or other electronic device to display, interpret, and process it. This includes documents (whether text, graphics, or spreadsheets) generated by a software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in electronic data 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.
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 to a class.

Term of Abbreviations	**What it stands for**
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 that all Information Assets are identified and that the business importance of those assets is established.
Data Custodian (DC)	They are local IG champions who have been nominated by their IAO, to support the Implementation of the IG agenda within their Teams.
Data Quality	Data Quality refers to the procedures and processes in place to ensure that data is accurate, up-to-date, free from duplication (for example, where two or more different records exist for the same individual), and free from confusion (where different parts of a individuals records are held in different places, and possibly in different formats).
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.
Place of Deposit	A Place of Deposit is a record office which has been approved by the National Archives for the deposit of public records in accordance with the Public Records Act 1958.
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to the 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	Record in the 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 the record of activity of a patients 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

Term of Abbreviations	What it stands for
	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
Taxonomy Management	A classification of documents into groups based on similarities of structures.

Appendix F Example Record Disposal Request Certificate

Section:	Name:	Date:
Title of Record (list all):		
Format (electronic/paper):		
Reason for disposal:		
Legal hold not placed upon these records:	None	
Method of destruction:		
Date of Disposal		
Authority:		
Not subject to current Information request:		

Appendix G Equality Impact Analysis

Equality Impact Analysis (SCW CSU Template) on the

Records Management Policy

1 What is it about? *Refer to the Equality Act 2010*

a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve

The Records Policy details how CCG will meet its legal obligations and NHS requirements concerning the management of Records.

b) Who is it for?

All staff

c) How will the proposal/policy meet the equality duties?

The policy will have no adverse effect on equality duties as it considers the management of records to be of equal status across all groups of people. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004

d) What are the barriers to meeting this potential?

There are no barriers.

2 Who is using it? *Consider all equality groups*

a) Describe the current/proposed beneficiaries and include an equality profile if possible

The policy is applicable to all.

b) How have you/can you involve your patients/service users in developing the proposal/policy?

Patients and service users have not been involved in developing the policy as this is an operational policy.

c) Who is missing? Do you need to fill any gaps in your data?

There are no gaps.

3 Impact *Consider how it affects different dimensions of equality and equality groups*

Using the information from steps 1 & 2 above:

a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is?

It is not anticipated that any adverse impact will be created. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004

b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified?

This is not applicable.

c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups?

This policy is equal across all groups.

d) Is further consultation needed? How will the assumptions made in this analysis be tested?

No.

4 So what (outcome of this EIA)? *Link to the business planning process*
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off ***(to be completed on approval of the policy)***

Name of person leading this EIA: **CSU IG Team**	Date completed: **12 February 2021** Proposed EIA review date: **March 2023**
Signature of director / decision-maker Name of director/decision-maker **Roshan Patel, Chief Finance Officer (Senior Information Risk Owner).**	Date signed: