University Hospital Southampton NHS
NHS Foundation Trust

Records Management Policy

Version: 6

Date Issued:	9 May 2018
Review Date:	19 April 2021
Document Type:	Policy

Contents		Page
Paragraph	Executive Summary	2
1	Introduction, Scope and Purpose	3
2	Definitions	4
3	Details of Procedure to be followed	5
3.1	Regulatory and legal framework	5
3.2	The Records Information Lifecycle	6
3.3	Record Creation	6
3.4	Handling and Using Records	7
3.5	Record Closure and Retention	9
3.6	Appraisal	10
3.7	Disposal	11
3.8	Additional Guidance on Specific Record Types	11
4	Roles and Responsibilities	13
5	Related Trust Policies	14
6	Communication Plan	14
7	Process for Monitoring Compliance/Effectiveness of this Policy	15
8	Arrangements for Review of this Policy	15
9	References	15

Appendices		Page
Appendix A	Record Creation and Filing Procedures	17
Appendix B	Medical Record Keeping Standards	21
Appendix C	List of Record Types listed in NHS retention Schedule	22

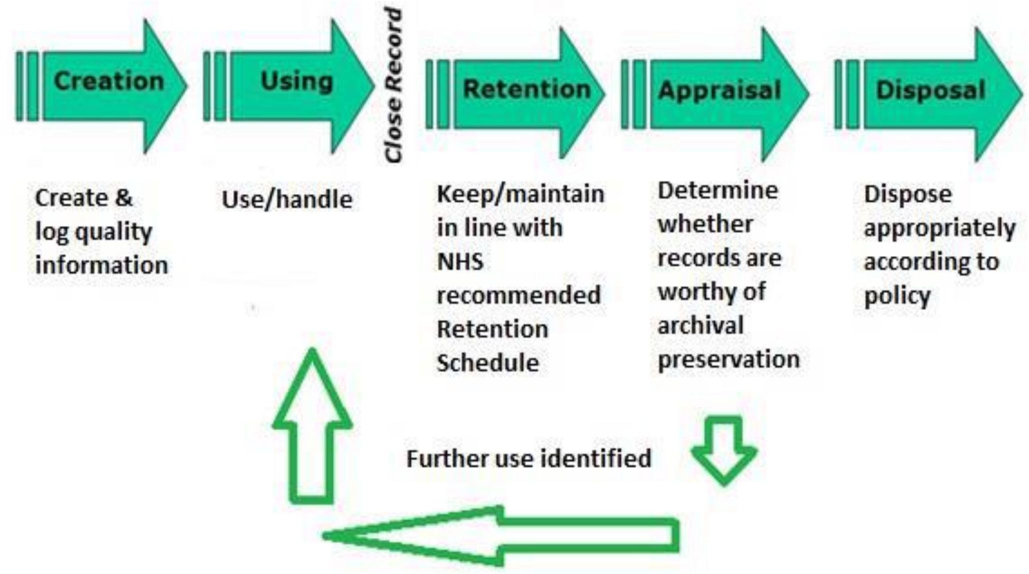
Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Executive Summary

1. There is a need to manage Trust records efficiently and effectively to support day to day operational and business activity and meet certain legal requirements. As we create and collect increasing amounts of information about our patients, staff and business activities it is vital that are able to organise, securely store and retrieve this information when required.
2. As we manage the incremental change from traditional/paper based record keeping to electronic/ digital systems we encounter new challenges, however the key principles of records management outlined in this policy continue to apply to these new storage mediums. Where different or additional guidance is required this is provided.
3. This policy is structured to provide staff with guidance on managing records through their life cycle from creation to disposal. Adherence to this guidance will support all aspects of Trust business and help the Trust comply with its duties as a public body subject to the Public Records Act (1958) and the Freedom of information Act (2000).
4. The Records/Information Life Cycle describes a regime designed to ensure information is managed from the point that it is created to the point that it either destroyed or permanently preserved as being of historical or research interest. The cycle is illustrated in this diagram:


Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log quality information
Use/handle
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of archival preservation
Dispose appropriately according to policy
Further use identified

5. In summary this policy:
   - Defines duties and responsibilities in regard to records management in the Trust
   - Outlines the key legal obligations and statutory provisions that apply to records created and used within the Trust
   - Provides a procedural Framework with guidance to encourage best practice in records management within the Trust
   - Describes the 'Information Life Cycle' and highlight best practice to be followed at each stage of the cycle from creation to disposal.

1. Introduction, Scope and Purpose

1.1 Introduction

1.1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal

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

1.1.3 Adherence to the guidance provided in this Policy will provide the Trust with a number of benefits including:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced costs.

1.1.4 This document sets out a framework within which Trust records can be managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.2 Scope

1.2.1 This policy applies to Trust records held in any format including:

- Paper
- Photographs slides and other images
- Microform microfich and microfilm
- Audio and video tapes, cassettes CD ROM etc
- Computerised records
- Scanned records
- Text messages and social media
- Websites and intranet sites that provide key information to patients

1.2.2 The majority of Trust members of staff will create records during the course of their day to day activity. Aspects of this policy will therefore apply to most members of staff, with specific responsibilities applying to department heads and managers for the management of local records created stored or held in their areas of responsibility.

1.2.3 At the time of publication of this policy preparations are being made to ensure the Trusts compliance with the implementation of the European Union General Data Protection Regulation (GDPR) in May 2018. To date no direct impact on the records procedures outlined in this policy has been identified as a consequence of the introduction of GDPR. As these preparations progress any identified changes required to records management policy and procedure will be made.

1.2.4 The Trust is also in the process of changing to a digital format of medical record recording and storage using the Onbase Electronic Document Management System (eDMS). An incremental roll out of the system to care groups has started but is at an early stage.

1.2.5 This policy makes an occasional reference to this significant change and the key principles for records management outlined in this policy (storage, retention etc) still apply to the records created and stored in Onbase.

1.2.6 As the incremental roll out of Onbase eDMS progresses and operational procedures are finalized this policy will be reviewed and the need for changes to be made or additional operational policies and procedures to be published will be agreed and implemented.

1.3 Purpose

1.3.1 The purpose of this policy is to:

- Define duties and responsibilities in regard to records management in the Trust
- Outline the key legal obligations and statutory provisions that apply to records created and used within the Trust
- Provide a procedural Framework with guidance to encourage best practice in records management within the Trust
- Describe the 'Information Life Cycle' and highlight best practice to be followed at each stage of the cycle from creation to disposal.

2. Definitions

Term	**Meaning Applied in this Policy**
Records Management	A set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.
Record	Information created, received and maintained as evidence and information by an organisation and person, in pursuance of legal obligations or in the transaction of business. (ISO Standard 15489-1:2016).
General Data Protection Regulation (GDPR)	European Union Directive which will replace the Data Protection Act (1998) in UK law, enforceable from 25th May 2018. Designed to harmonise data protection regulation across the European Union.
Electronic Document Management System (eDMS)	A software program/system that manages the creation, storage and control of documents electronically.
Information Life Cycle	A term that describes a controlled regime in which information is managed from the point that it is created to the point that it either destroyed or permanently preserved as being of historical or research interest.
Public Authority	An organisation within the categories listed in Schedule 1 to the Freedom of information Act defined as 'a body that appears to be exercising functions of a public nature or who are providing, under contract with a public authority, any service whose provision is a function of that authority. The Trust is a Public Authority.
Metadata	Data that describes information about other data. e.g. author and creation date of a record are elements of its metadata.
Record Classification Scheme	Means by which a record keeping system arranges or organises records to enable appropriate management controls to be applied and support accurate retrieval of information. e.g. a filing index.

Public Records	Administrative and departmental records belonging to Her Majesty, in the UK or elsewhere, in right of Her Majesty's Government, and in particular records of or held in any government department and records of offices, commissions or other bodies under HMG in the UK. (Public Records Act 1958). All Trust records are public records subject to the Public Records Act (1958)
Data Subjects	An individual who is the subject of personal data.
Patient Administration System (PAS)	Electronic system used to hold non clinical details about Trust patients (demographics, GP details, contacts etc).
Electronic Clinical Record Tracking (eCRT)	A module of the Trust PAS used to record the movement of patient Health Record Folders within UHS and partner organisations.
Record closure	The process followed to make a record inactive when it has ceased to be in active use other than for reference purposes.
Record retention	The process of keeping a record for a period of time for administrative, legal, fiscal, historical, or other purposes.
Record appraisal	The process of deciding what to do with a record when the business use has ceased. The outcome of record appraisal will be either: destroy/delete, retain for a further period or transfer to a Place of Deposit.
The National Archives (TNA)	A non-ministerial department, and the official archive and publisher for the UK Government, and for England and Wales. TNA publishes advice and guidance on information and records management.
Place of Deposit (POD)	Record Archive storage location appointed by the Secretary of State for Culture Media and Sport. Usually a public archive service provided by a Local Authority.
Corporate Records	Records of business processes such as accounting, procurement, staff management and estates maintenance. In NHS organisations this term covers all records that are not patient/care records.
Permanent preservation	A process followed to place a record in an archive storage location allowing public access to records of historical administrative or local importance.
Record Disposal	The destruction, deletion or transfer for permanent preservation of a closed record
British Standard 10008-2014 Evidential Weight and Legal Admissibility of Electronic Information	The British Standard that outlines best practice for the implementation and operation of electronic information management systems, including the storage and transfer of information.
Information Governance	An umbrella term relating to the processes and systems used by organisations to manage the information they hold. In the context of the NHS, it specifically refers to the processes and procedures used to ensue confidentiality, security and accuracy of information.

3. **Details of Procedures to be Followed**

3.1 Regulatory and Legal Framework

3.1.1 Under the terms of the Public Record Act 1958 all records created in the Trust are regarded as public records. The act imposes a statutory duty on the Trust to make arrangements for the safe keeping and eventual disposal of records. The ownership and copyright of records created within Trust lies with the Trust and not the individual who has created them.

3.1.2 As a Public Authority subject to the Freedom of Information Act the Trust has a duty to follow the Code of Practice for Records Management published by the Lord Chancellor in accordance with section 46 of the FOIA. The code provides guidance to public authorities on keeping, managing and destroying records.

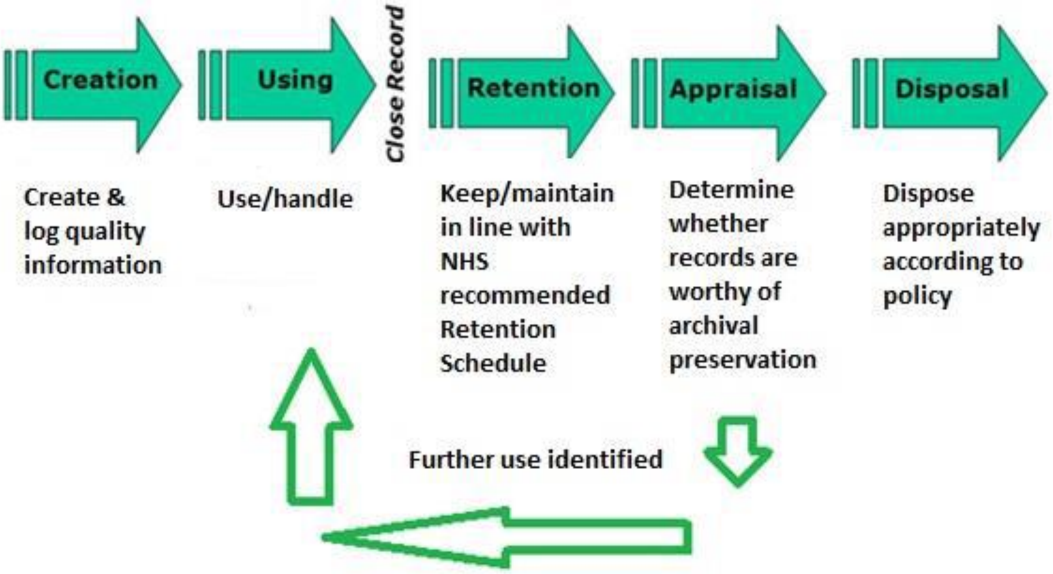
3.1.3 The Data Protection Act sets in law how personal and sensitive information may be processed and largely influences the way we handle care records. Further guidance on the confidentiality aspects of record keeping is provided in the NHS Confidentiality Code of Practice and the Trust Data Protection and Confidentiality Policy.

3.1.4 The Records Management Code of Practice for Health and Social Care 2016 provides records management guidance for NHS and Social Care organisations based on current legal requirements and professional best practice. The Trust is committed to following the guidance issued in the code of practice and the procedures outlined in this policy are largely based on the guidance included in this Code of Practice.

3.2 <u>The Records Information Lifecycle</u>

3.2.1 The records or information lifecycle is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it either destroyed or permanently preserved as being of historical or research interest. The cycle is illustrated in figure 1

Figure 1. The Information Lifecycle


Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log quality information
Use/handle
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of archival preservation
Dispose appropriately according to policy
Further use identified

3.2.2 Procedural guidance associated with each stage of the cycle is included in subsequent sections

3.3 <u>Record Creation</u>

3.3.1 ISO 15489-1:2016 Information and Documentation – Records Management describes the characteristics of 'Authoritative Records' as being authentic, reliable integral and useable. Table 1 below expands on these definitions.

Table 1. Record Characteristics

Record Characteristic	How to Evidence
Authentic	It is what it purports (claims) to be To have been created or sent by the person purported to have created or sent it and To have been created or sent at the time purported.
Reliable	Full and accurate record of the transaction/activity or fact Created close to the time of transaction/activity Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	Complete and unaltered Protected against unauthorised alteration Alterations after creation can be identified as can the persons making the changes.
Useable	Located, retrieved, presented and interpreted The context can be established through links to other records in the transaction/activity.

3.3.2 By organising records in a file system or classification scheme elements of 'Metadata' are associated with each record which helps maintain the characteristics described above. Metadata in its simplest form would identify the creator, creation date and subject of a record but can be expanded to include additional information such as destruction date, identifiers and accessibility.

3.3.3 Classification schemes can be a simple arrangement of files and folders on a Network drive increasing in sophistication up to a full blown Electronic Document and Records Management System such as the Onbase edMS being introduced to store patient records in the Trust.

3.3.4 All Trust records should be stored within an appropriate classification/filing system after creation. This will ensure they remain secure and accessible from the outset and be available to support Trust business activity.

3.3.5 A more comprehensive guide for users covering the creation and filing of records is attached at **Appendix 1**.

3.4 Handling and Using Records

3.4.1 Record Keeping

3.4.1.1 When completing entries in or creating any form of records the following general guidance should be applied:

- Be factual, consistent and accurate
- Write clearly and in such a way that text cannot be erased
- Write in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read.

3.4.1.2 Healthcare professionals may be subject to additional record keeping codes of practice set by their professional bodies. The Academy of Medical Royal Colleges has published a set of generic medical record keeping standards which are reproduced at **Appendix 2**. All entries in Trust care records should conform to these standards.

3.4.1.3 Rights granted to members of the public by the Freedom of Information Act and to patients and staff under the Data Protection Act can result in copies of corporate records being placed in the public domain and data subjects obtaining copies of records containing information about them. Providing record entries are factual and accurate and personal records do not include any unnecessary and/or derogatory comments record disclosure should not create any additional issues.

3.4.2 Confidentiality and Access

3.4.2.1 All Trust records are public records and thus are subject to a number of statutory provisions regarding confidentiality, access and disclosure. Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

3.4.2.2 Specific guidance on patient confidentiality issues is provided in the Trust Data Protection and Confidentiality Policy. Further advice on all aspects of patient confidentiality and the application of the Data Protection Act (1998) on the way we handle records in the Trust can be obtained from the Trust Information Governance Manager.

3.4.2.3 The Data Protection Act (1998) makes provision in law for ‘data subjects’ (e.g. patients and members of staff) to obtain copies of otherwise gain access to information held about them. The Trust Access to Records Policy covers this aspect of records management and further advice on the procedure can be obtained from the Trust Information Governance manager.

3.4.2.4 In 2000 the government introduced the Freedom of information Act providing members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of this legislation is to make it possible for people to obtain copies of a wide range of Trust records that in the past would have remained confidential. The Trust Freedom of Information Policy covers this aspect of records management and further advice on the procedure can be obtained from the Trust Information Governance manager.

3.4.3 Record Tracking

3.4.3.1 Ideally the movement and location of all records should be controlled to ensure that a record can be retrieved at any time and there is an auditable trail of record transactions. This is best achieved using some form of record tracking system to record the movement of records between locations.

3.4.3.2 It is the policy of the Trust that patient health record folders are tracked using the PAS record tracking component (electronic casenote record tracking e-CRT.) Users are provided with training to use e-CRT prior to being granted access to the system.

3.4.3.3 While electronic records do not require tracking as such, control must be exercised when hard copies are produced. If separate clinical casenotes are produced from electronic systems to form a filing system individual record movements should be tracked to aid retrieval and avoid loss of data.

3.4.3.4 For most areas, where movement of records is restricted, paper based systems may be employed, using registers or tracer cards to record the relevant information.

3.4.3.5 When making arrangements to move records which contain personal or sensitive information to destinations external to the Trust (including archive storage) consideration needs to be given to security and confidentiality and a means of dispatch chosen that affords an adequate level of security. (See Trust Data Protection Policy for further guidance.)

3.4.4 Record Storage

3.4.4.1 When not required for operational purposes records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

3.4.4.2 Records should be stored in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. When evaluating the suitability of a location for record storage the following points should be considered:

- Environment. Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records? i.e. excessive dust, damp, restricted access.
- Security. Is the level of security offered by the location acceptable for the type of record being stored?
- Ease of Access. Can records be easily located and retrieved? Some restrictions on access may be acceptable for records that are not frequently recalled.
- Layout. Consideration should be given to the design of the storage location to ensure the most cost effective use is made of the space available.

3.4.4.3 External storage companies provide an alternative to local storage and in the short term can prove a cost effective alternative in areas where record storage space is at a premium. The Trust has negotiated a contract for external record storage with a Restore, a national provider with storage premises located a few miles East of Southampton. Advice on external storage options and alternative strategies such as archiving records to digital formats can be obtained from the Trust records manager.

3.4.4.4 A comprehensive record should be maintained of any records sent for commercial storage including a proposed date for review/destruction. A mechanism for reviewing these records for disposal should be developed and implemented to ensure records are not retained longer than necessary.

3.4.4.5 Digital information should be stored in such a way that throughout the lifecycle it can be recovered in an accessible format. Over time such changes as migration to new formats can cause links to other documents and embedded documents to fail to open impacting the integrity of the record. Any changes to the electronic storage systems used to hold Trust records should only take place after full consideration of the impact on the records held and successful testing of retrieval of transferred records from the new version/system.

3.5 Record Closure and Retention

3.5.1 A record should be closed when the business use for that record ceases. Following closure NHS records are subject to a minimum period of retention. The length of the retention period varies by record type and is based on legal and regulatory requirements and the assessed importance of and likely need to access the type of record.

3.5.2 Certain types of corporate records (e.g. finance, meeting records etc) will follow annual cycles with existing records closed following year end and new records created for the new year (calendar or financial).

3.5.3 Paper record folders should be clearly marked with the date of closure and planned review/disposal date. Closed records in electronic storage systems should hold this information as part of the record's metadata and/or the record moved to another area of the system reserved for closed records.

3.5.4 For patient care records the recognised date of record 'closure' is normally the date of the patient's last attendance for treatment. Where a patient has died subsequent to treatment at the Trust the retention period applicable to deceased patient records (8 years) may be applied from the date of death, if this results in a shorter retention period.

3.5.5 Minimum retention periods for NHS and Social Care records are set out in Appendix 3 of the Code of Practice which can be accessed via this link: https://digital.nhs.uk/codes-of-practice-handling-information
Periods of retention between 6 months and 20 years are listed for NHS record types organised by functional groups. A list of the NHS record types with minimum retention periods listed in the Code of practice is reproduced at **Appendix 3**.

3.5.6 The majority of adult patient health records are subject to a minimum retention period of 8 years. Health records for Children, Obstetric records, mental health (including psychology) records, and records recording treatment for cancer are all subject to longer periods of retention.

3.5.7 The period of retention is measured from the start of the calendar year following the record closure date. e.g. record closed 1 July 2017 subject to 5 year retention period. Period starts 1 Jan 2018 and ends 31 Dec 2022.

3.5.8 The code of practice lists minimum periods of retention and in most cases it will be appropriate to destroy records immediately once the period has expired. Retention beyond the recommended period is permitted with good reason but if personal data is held 'longer than necessary' the Trust may breach a provision of the Data Protection Act.

3.5.9 The Public Records Act 1958 states no public record can be retained after closure for a period in excess of 20 years without permission from the Sec of State for culture Media and Sport. However, a legal exemption applies for individual NHS staff and patient records to meet the extended (20 years plus) periods of retention listed for these records in the Code of Practice.

3.6 Appraisal

3.6.1 When the minimum retention period for a record or set of records has passed it should be subject to an appraisal. The purpose of the appraisal process is to:

- Identify records of public interest worthy of permanent preservation by transfer to The National Archives or a local Place of Deposit.
- Identify records to be retained for a longer period
- To confirm that records not meeting above criteria should be deleted or destroyed.

3.6.2 A small percentage of Trust records will meet the criteria for selection for permanent preservation. The preservation of a small subset of key records is designed to enable the public to understand the working of the Trust and the impact on the population it serves and to preserve information likely to have long term research value.

3.6.3 The Code of Practice includes guidance on the records that should be considered for preservation in the schedule of minimum retention periods. The suggestions for consideration include Trust Board and other key committee papers, key policies and strategies and records of major building works.

3.6.4 The process of selection of key corporate records for permanent preservation will be managed by the Trust Records manager and the Director of Corporate Affairs who will agree with the Trust's local Place of Deposit (POD), Southampton City Archives, which Trust records merit transfer.

3.6.5 Clinical records are problematic to preserve permanently in an archive and due to confidentiality issues personal health records cannot normally be accessed by the public for considerable periods of time following transfer. This does not prevent appropriate sets of clinical records being considered for permanent preservation and the Code of Practice provides some specific guidance on this process.

3.7 Disposal

3.7.1 Following appraisal any records not selected for permanent preservation or a longer retention period should be disposed of. No information should be destroyed if it is the subject of a request under the DPA and/or FOIA or any other legal process, such as an inquest following a death.

3.7.2 Paper records should be destroyed securely through a local process of cross cut shredding or using the Trust confidential waste disposal service or other similar secure disposal service.

3.7.3 Destruction of digital information is more challenging. At present there are two ways of permanently destroying digital information and these are either: overwriting the media a sufficient number of times or the physical destruction of the media. Further advice about the destruction of digital records can be obtained from the Trust Informatics service.

3.7.4 Where decisions are made to destroy/dispose of a series or bulk number of Trust records a record of the decision and the details of the records disposed of should be maintained.

3.8 Additional Guidance on Specific Record Types

3.8.1 E-Mail

3.8.1.1 Personal e-mail accounts tend to be structured according to personal preference and the data stored is not searchable and organised in a systematic way, making e-mail accounts unsuitable for record storage purposes.

3.8.1.2 E-mail accounts should not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents. E-mails or documents distributed by e-mail that need to be retained as Trust records should be copied to the appropriate paper or electronic registered file system and the e-mail copy destroyed as soon as practicable.

3.8.1.3 Where email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral - for example an email approving a business case must be saved with the business case file. Emails that are the sole record of an event or issue, for example an exchange between a clinician and a patient, should be copied in to the relevant clinical record rather than being simply deleted.

3.8.2 Scanned Records

3.8.2.1 Where paper records are scanned, 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.

3.8.2.2 Complying with the standard, '*BS 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information*' provides one method of ensuring and demonstrating that electronic information remains authentic. The scanning of Trust patient records for inclusion in the Onbase eDMS patient record system is being carried out in accordance with this standard.

3.8.2.3 For smaller scale local record scanning projects compliance with the full scope of BS 1008 will not be the appropriate methodology. Methods that can be employed to ensure that scanned records can be considered authentic include:

- A written procedure outlining the process to scan, quality check and any destruction process for the paper record
- Evidence that the process has been followed
- An audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- Fix the scan into a file format that cannot be edited such as Portable Document Format (PDF).

3.8.2.4 Providing scanning is carried out to an acceptable standard with an element of quality assurance included in the process it is Trust policy and normal practice that original documents should be destroyed after scanning. This prevents issues with two versions of the same record existing (original and scanned) and maximises the benefits accruing from scanning paper records.

3.8.2.5 There may be some local exceptions to this practice with appropriate justification.

3.8.3 Staff Records

3.8.3.1 Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the paperwork collected through the recruitment process and this will be expanded over time with additional material added by line managers.

3.8.3.2 Upon termination of contract, records must be held up to and beyond the staff member's statutory retirement age. On contract termination line managers should return the employees file to HR department for retention until the employee's 75th birthday or 6 years after leaving whichever is the longer. To reduce the burden of storage a summary record may be prepared and held.

3.8.4 Records of non NHS Funded Patients

3.8.4.1 Records of individuals who are not NHS funded held in the Trust record keeping systems must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

3.8.5 Adopted Persons Health Records

3.8.5.1 The records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

3.8.5.2 Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Care must be exercised when disclosing records of adopted patients because of the heightened risk of accidental disclosure.

3.8.5.3 It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the patients GP will initiate any change of NHS number or identity if it was considered appropriate to do so, following the adoption. The Trust would then make changes to its own records in line with that initiated by the patient's GP.

3.8.6 Health Records of Transgender Patients

3.8.6.1 Patients considering or undergoing gender identity change may ask for changes to their name they are known by to be made and in most cases the Trust will agree to such a request.

3.8.6.2 A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004.

3.8.6.3 The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient.

3.8.6.4 Except in a limited set of circumstances it is an offence under the gender recognition act to disclose without consent information that would identify that a person has undergone a gender identity change.

3.8.6.5 The key to the successful management of records in these circumstances is to discuss with the patient their choices and agree what they wish to happen in respect to their health record. If a new health record is being created there is a need to identify which records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

4. Roles and Responsibilities

4.1 Chief Executive

4.1.1 As accountable officer the Chief Executive is responsible for the overall leadership and management of the Trust and its performance in terms of service provision, financial and corporate viability, ensuring that the Trust meets all its quality and safety, statutory and service obligations and for working closely with other partner organisations. The CEO delegates aspects of this responsibility to relevant Executive Directors according to their organisational portfolios.

4.2 Director of Transformation and Improvement

4.2.1 The Director of Transformation and Improvement is the appointed Executive Director with responsibility for Information Governance including records management and is the Trust Senior Information Risk Owner (SIRO).

4.2.2 The SIRO is responsible for managing information risk in the Trust and will implement and lead the NHS Information Governance risk assessment and management processes within the Trust and advise the Board on the effectiveness of information risk management.

4.3 Caldicott Guardian

4.3.1 The Trust Caldicott Guardian is the Director of Nursing who has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Trust Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.3.2 The duties and responsibilities of the Trust Caldicott Guardian are outlined in the Trust Confidentiality and Data protection Policy.

4.4 Trust Records Manager

4.4.1 The Trust Records Manager is responsible for ensuring that this policy is implemented and that the records management system and associated processes are developed, co-ordinated and monitored.

4.4.2 The Trust Records Manager is also responsible for the overall development and maintenance of health records management practices and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

4.5 Local Managers

4.5.1 The responsibility for local records management is devolved to divisional, care group and department heads whom retain overall responsibility for the management of records generated by their activities, i.e. for ensuring that records created within their unit are managed in a way which meets the aims of the Trust's records management policy and associated procedures.

4.6 Clinical Leads and Matrons

4.6.1 Clinical leads in all professions have a responsibility to ensure clinical staff they manage who contribute to patient health records are adequately trained in record keeping and are aware of and adhere to the standards for record keeping outlined in this policy.

4.7 All Staff

4.7.1 Members of Staff who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

4.7.2 Staff who make entries in medical records should do so in accordance with the clinical record keeping standards published in this policy. In addition Royal Colleges and other professional bodies publish record keeping guidance for clinical staff and it is the responsibility of clinical staff to ensure they keep up to date with and adhere to relevant legislation, case law and national guidance.

5. Related Trust Policies

5.1 The following Trust policies overlap with or relate to matters covered in this policy

- Information Governance Policy
- Data Protection and Confidentiality Policy
- Freedom of Information Policy
- Access to Records Policy
- Subject Access Policy
- IM&T Security Policy
- Incident Management Policy
- Patient Information and Corporate Identity Policy
- Web Publishing Policy

6. Communication Plan

6.1 The publication of this updated policy will be highlighted to staff via an article on the news section of ‘Staffnet’, the Trust intranet. The article will draw attention to the key changes made to the previous policy version.

6.2 A copy of this policy will be available for staff to access via the policies section of Staffnet and links to the policy will also be provided within the records management section of the Information Governance pages of Staffnet.

6.3 Elements of record training and procedure form part of the annual training for information governance (now known as data security training) which forms part of the Trusts annual mandatory training requirement.

7. Process for Monitoring Compliance and Effectiveness

7.1 The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures we get things right for patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be assessed or measured.

Key aspects of the procedural document that will be monitored:

What aspects of compliance with the document will be monitored	What will be reviewed to evidence this	How and how often will this be done	Detail sample size (if applicable)	Who will co-ordinate and report findings (1)	Which group or report will receive findings
Compliance with Record handling best Practice and guidance	Incidents reported with record related cause codes	Ongoing monitoring carried out by local governance leads and Trust Records Manager	N/A	Local governance leads and Trust Records Manager	Serious breaches will be reported to the Information Governance Steering Group
Medical records procedures for retrieval and tracking	Sample or record movements recorded on Trust PAS	Quarterly audit carried out by Medical Records Manager	25 records per quarter	Medical Records Manager	Information Governance Steering Group
Medical Record Keeping Standards	Entries in sample of Trust inpatient medical records	Annual Audit as part of Trust Clinical Audit programme.	100 records plus	Audit managed by Trust Clinical Audit Manager and local Divisional audit leads	Clinical Effectiveness Steering Group

Where monitoring identifies deficiencies actions plans will be developed to address them.

8. Arrangements for Review of the Policy

8.1 This policy will be subject to formal review three years after publication unless significant changes in legislation or NHS guidance dictate an earlier review. Minor updates will be made as and when required.

8.2 If as a result of the full adoption of GDPR legislation into UK law on the 25th May 2018 a further amendment to this policy is required then this will be carried out. See para 1.2.3 above.

9. References

Public Records Act (1958)
Freedom of Information Act (2000)
Data Protection Act (1998)
General Data Protection Regulation
Records Management Code of Practice for Health and Social Care 2016
Academy of Medical Royal Colleges' Standards for the clinical structure and content of patient records
Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act (2000).
The National Archives
BS 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information

Appendices

A. Record Creation and Filing Procedures
B. Medical Record Keeping Generic Standards
C. Categories of Records listed in NHS Retention Schedule

Appendix A to Records Management Policy

User Guide to Record Creation

Introduction

1. This guide primarily covers records created for non care purposes as the procedure for creating and filing patient records is part of the training given to users of the Patient Administration System. The key principles apply to all records however.
2. Although most records in the Trust are created and stored electronically some paper based record keeping systems are still in use. Most of the guidance provided in this document can be applied to both forms of records but where this is not the case users will need to exercise judgment when applying the guidance.
3. Common types of documents such as letters, meeting minutes, Job Descriptions etc should be always be created using the Trust Word Templates set up for these document types. When creating documents staff should take note of the guidance about document style contained in the Trust Patient Information and Corporate Identity Policy available on the Trust Intranet.
4. All records created in the Trust should be included in a record keeping filing system and be given a unique title or name to identify it. When creating records users need to consider the need for privacy markings and version control. The guidance set out in the following sections addresses these requirements and provides guidance in their application.

Record Filing Systems

5. Records created in both electronic or paper form should be organised in some form of registered fling system so they can be easily located when needed and documents of a similar or linked nature are kept together. Filing systems can be created and organised using a variety of methods. Probably the most common method is a simple alphanumeric system whereby records are grouped together in folders that are given unique names. The folders are then organised/ordered in alphanumeric fashion in draws/cabinets (paper records) or within Trust HQ/Divisional/Care Group hard Drives (electronic records)
6. When designing and developing filing systems the following points should be considered:

   a. Retain control and continuity by restricting the number of staff who can create new folders in the system.
   b. Organise folders and sub folders in a logical manner that will make sense to those who need to access records within them. e.g. organised by function or teams.
   c. Give each folder a clear title that describes the contents within. e.g. '*MeetingsDiv Board2009', 'ComplaintsPatients200804to200906*. Avoid names like '*General', 'Miscellaneous'* or personal titles like '*Jane's Folder'*. (See next section for more details on file names)
   d. Within folders records are normally filed in chronological order by date of creation or receipt. It is good practice to clearly stamp on the front or all documents received the date of receipt.
   e. Folders in hard copy filing systems should be marked with the date the folder was opened and when closed the date of closure. When files are closed the date when the folder should be reviewed prior to disposal (usually at the end of the minimum retention period) should be added. In electronic filing systems these pieces of information can often be added to the metadata for the folders created.

f. A regular programme of reviews should be established to consider the need for closure and disposal of records/folders. The frequency of these reviews will largely depend on the size and growth rate of the filing system.

g. A summary of the responsibilities, organisation and conventions used for each filing system should be set out in a document that is made available to all those who access the system.

Folder and File Naming/Referencing Conventions

4. Names for folders and documents should be kept as short as possible whilst also being meaningful. Long file names create long file paths and links which increase the likelihood of error and are more difficult to remember. Avoid using personal names and codes and abbreviations that are not commonly understood.

e.g. use ‘*H&SCtteeTOR.doc’* in preference to
‘*Health_&_Safety_Comittee_Terms of_Reference.doc’*

5. When creating sub folders and files within electronic filing systems there is no need to include in the file name descriptive information already contained in the parent folder as this will already form part of the filename/file path.

e.g. use: *‘/.../DivBoard/**agenda20100210***’
not: *‘/.../DivBoard/**DivBoardagenda20100210***

6. Avoid using spaces and underscores in file names. Some software packages have difficulty recognising file names with spaces. Use capital letters to delimit words.

e.g. use ‘*AuditMeetingsAgendas.doc’* in preference to ‘*Audit_Meetings_Agendas.doc*’

7. When using a number in a file name always give it as a two digit number so that when it is displayed in the file directory in alphanumeric order it will be ranked in the correct order. Organised alphanumerically ‘*ab2’* will be listed after ‘*ab10’.*

e.g. V01, V02, V03 etc not V1, V2, V3.

8. If using a date in the file name always state the date ‘back to front’ and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY. Writing dates in this way will present the records in chronological order in the file list with the latest record at the end of the list.

e.g. use ‘*20100201agenda.doc’* not ‘*1Feb2010Agenda.doc’*

9. The elements of the file name should be ordered in the most appropriate way to retrieve the record. If records are retrieved by date the date element should appear first, if retrieved according to description then this should appear first.

e.g. ‘*20100201agenda.doc’* (date retrieval) or ‘*agenda20100201’* (subject retrieval).

Protective Marking of Documents

10. The NHS has agreed a scheme of classification using two privacy markings;

a. **NHS CONFIDENTIAL**. This classification should be used for paper and electronic documents containing personal identifiable clinical or NHS staff information and other sensitive information the compromise of which could lead to serious consequences for the Trust. The marking should be included at the top centre of every page of the document and documents so marked should be held and transported securely at all times. (The term **NHS CONFIDENTIAL** should never be used on correspondence to a patient.)

b. **NHS RESTRICTED**. This classification should be used to mark all other sensitive information. Documents marked **NHS RESTRICTED** may also be endorsed with a suitable descriptor indicating the reason for the classification. A list of these descriptors is shown in the table below. The marking should be included at the top centre of every page of the document and documents so marked should be kept in lockable containers.

11. When classifying documents regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given to classifying documents that would be normally be published or disclosed on request.. Protective markings should wherever possible only be applied to documents that would be exempt from disclosure.

Table 1 Categories of **NHS RESTRICTED** Documents

Category	Definition
Appointments	Concerning actual or potential appointments not yet announced
Barred	Statutory prohibition on disclosure exists or disclosure would constitute contempt of court.
Board	Documents considered by an organisation’s Board of Directors, initially in private.
Commercial	Where disclosure would be likely to damage a third party commercial undertaking’s processes or affairs
Contracts	Concerning tenders
For Publication	Where it is planned that the information will be published at a future date.
Management	Concerning policy and planning affecting the interests of a groups of staff
Personal	Concerning matters personal to the sender or recipient
Policy	Issues of approach or direction on which the organisation needs to take decision.
Proceedings	Information the subject of or concerned in a legal action or investigation

Version Control

12. Document version control allows the management of multiple revisions of the same document and is important as it enables users to distinguish between different versions of a document and to identify if the document they are using is the latest version. When several people are collaborating on a document version control will help identify when any changes have been made by any of the collaborators.
13. When creating a document where more than one version does or is likely to exist a unique version number should be included in the document name and clearly

displayed in the document.

14. Consecutive whole numbers should be used to identify major revisions to documents. i.e. version 01, version 02 etc. The addition of the word Draft or Final at the end of the file name can be used to indicate the status of the document

e.g.	*‘/...AnyRecordV01Draft.doc’*	First draft version
	‘/.../AnrrecordV02Draft.doc’	Second draft version
	‘/.../AnyRecordV03Final.doc’	3rd and final version

15. Where documents may be subject to many changes smaller revisions can be indicated by using version numbers with decimal points to indicate major and minor changes.

e.g.	*‘/.../AnyrecordV01.1doc’*	First Version
	‘/.../AnyrecordV02.1doc’	Second version with major change
	‘/.../AnyrecordV02.2doc’	Second Version with minor change

16. In key documents subject to a period of development it is useful to display at the front of the document after the title page, a version control table showing the development history of the document and the version changes that have been applied. An example is shown below. It is also useful to display the document version number in the footer section of every page so readers can be clear they are viewing the latest version.

Date	Author	Description	Version
01 Jan 2009	PW	Initial Draft circulated for comment.	0.1
10 Jan 2009	PW	Revised draft version incorporating comments from review group	0.2
31 Jan 2009	PW	Final Draft for approval ISSG	1.0
09 Sep 2009	AJ	Major update following publication of new Trust Strategy	2.0
12 Feb 2010	AJ	Minor changes incorporating new Trust structure and organisation	2.1

Appendix B to Records Management Policy

AoMRC Medical Record Keeping Standards

Standard Number	Description
1	The patient's complete medical record should be available at all times during their stay in hospital
2	Every page in the medical record should include the patient's name, identification number (must include NHS number, may include local ID) and location in the hospital
3	The contents of the medical record should have a standardised structure and layout
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma
6	Every entry in the medical record should be dated, timed (24 hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated and timed[27]
7	Entries to the medical record should be made as soon as possible after the event to be documented (for example change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded
8	Every entry in a medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
9	On each occasion a transfer of care occurs, the consultant responsible for the patient's care will change the name of the responsible consultant and the date and time of the agreed transfer of care
10	An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for long-stay continuing care, the next entry should explain why
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital
12	Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney

Appendix C to Records Management Policy

Categories of Records with Minimum Periods of Retention Listed in Records Management Code of Practice for Health and Social Care 2016

1. Care Records with standard retention periods

- Adult health records
- Adult social care records
- Children’s records including midwifery, health visiting and school nursing
- Electronic Patient Records Systems
- General Dental Services records
- GP patient records
- Mental Health records
- Obstetric records, maternity records and antenatal and post natal records

2. Care Records with non-standard retention periods

- Cancer/oncology - the oncology records of any patient
- Contraception, sexual health, family planning and Genito-Urinary Medicine (GUM)
- Human Fertilisation & Embryology Authority (HFEA) records of treatment provided in licenced treatment centres
- Medical record of a patient with Creutzfeldt-Jakob disease (CJD)
- Record of long term illness or an illness that may reoccur

3. Pharmacy Records

- Information relating to controlled drugs
- Pharmacy prescription records - see also Information relating to controlled drugs

4. Pathology Records

- Pathology Reports/Information about specimens and samples

5. Event & Transaction Records

- Blood bank register
- Clinical Audit
- Chaplaincy records
- Clinical Diaries
- Clinical Protocols
- Data sets released by HSCIC under a data sharing agreement
- Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media
- Equipment maintenance logs
- General Ophthalmic Services patient records related to NHS financial transactions
- GP temporary resident forms
- Inspection of equipment records
- Notifiable disease book
- Operating theatre records
- Pathology Reports/Information about Specimens and samples
- Patient Property Books
- Referrals not accepted

- Requests for funding for care not accepted
- Screening, including cervical screening and information where no cancer/illness is detected
- Smoking cessation
- Transplantation Records
- Ward handover sheet

6. Telephony Systems & Services Records - 999 phone numbers, 111 phone numbers, ambulance, out of hours and single point of contact call centres.

- Recorded conversation which may later be needed for clinical negligence purpose
- Recorded conversation which forms part of the health record
- The telephony systems record

7. Births, Deaths & Adoption Records

- Birth Notification to Child Health
- Birth Registers
- Body Release Forms
- Death - cause of death certificate counterfoil
- Death register information sent to General Registry Office on monthly basis
- Local Authority Adoption Record (normally held by the local authority children's services)
- Mortuary records of deceased
- Mortuary Register
- NHS medicals for adoption records
- Post Mortem records

8. Clinical Trials & Research Records

- Advanced Medical Therapy Research Master File
- Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014
- European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states' area
- Research data sets
- Research Ethics Committee's documentation for research proposal
- Research Ethics Committee's minutes and papers

9. Corporate Governance Records

- Board Meetings
- Board Meetings (Closed Boards)
- Chief Executive records
- Committees Listed in the Scheme of Delegation or that report into the Board and major projects
- Committees/Groups/sub-committees not listed in the Scheme of Delegation
- Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media
- Incidents (serious)

- Incidents (not serious)
- Non-Clinical Quality Assurance Records
- Patient Advice and Liaison Service (PALS) records
- Policies, strategies and operating procedures including business plans

10. Communications

- Intranet site
- Patient information leaflets
- Press releases and important internal communications
- Public consultations
- Website

11. Staff Records & Occupational Health

- Duty Roster (Staff providing Care)
- Exposure monitoring information
- Occupational Health Reports
- Occupational Health Report of Staff member under health surveillance
- Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses
- Staff Record
- Staff Record Summary
- Timesheets (original record)
- Staff Training records

12. Procurement

- Contracts sealed or unsealed
- Contracts - financial approval files
- Contracts - financial approved suppliers' documentation
- Tenders (successful)
- Tenders (unsuccessful)

13. Estates

- Building plans and records of major building work
- CCTV
- Equipment monitoring and testing and maintenance work where asbestos is a factor
- Equipment monitoring and testing and maintenance work
- Inspection reports
- Leases
- Minor building works
- Photographic collections of service locations and events and activities
- Radioactive Waste
- Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhydrin Test
- Surveys

14. Finance Records

- Accounts
- Benefactions
- Debtor records cleared

- Debtor records not cleared
- Donations
- Expenses
- Final annual accounts report
- Financial records of transactions
- Petty cash
- Private Finance initiative (PFI) files
- Salaries paid to staff
- Superannuation records

15. Legal, Complaints & Information Rights

- Complaints case file
- Fraud case files
- Freedom of Information (FOI) requests and responses and any associated correspondence
- FOI requests where there has been a subsequent appeal
- Industrial relations including tribunal case records
- Litigation records
- Patents / trademarks / copyright / intellectual property
- Software licences
- Subject Access Requests (SAR) and disclosure correspondence
- Subject access requests where there has been a subsequent appeal

Records Management Policy **Version: 6**

Document Monitoring Information

Approval Committee:	Information Governance Steering Group
Date of Approval:	15 March 2018
Ratification Committee:	Policy Ratification Group
Date of Ratification:	19 April 2018
Signature of ratifying Committee Group/Chair:	Amanda Lowe, Associate Director- Corporate Affairs
Lead Name and Job Title of originator/author or responsible committee/individual:	Paul McMahon, Trust Records Manager
Policy Monitoring (Section 6) Completion and Presentation to Approval Committee:	Medical records audit results considered at IGSG meetings during 2017/18. Medical record keeping audit to be presented to QGSG in March 2018.
Target audience:	All staff
Key words:	Records; records management; information; governance; record keeping; storage; retention; information; documents; archive; archiving; appraisal; filing; tracking.
Main areas affected:	Trust wide
Summary of most recent changes if applicable:	Formal review and update. Changes made to layout and structure. Guidance set out in new NHS Code of Practice incorporated. GDPR compliant document.
Consultation:	Div Governance leads. Exec director for Informatics. Clinical audit Manager. Associate Medical Director (Dr. Waller) Associate Director of Corporate affairs. Head of Informatics. Information Governance Manager. Medical Records Manager.
Equality Impact Assessment completion date:	15 March 2018
Number of pages:	26
Type of document:	Policy, Level 1
Does this document replace or revise an existing document	Records Management Policy v 5.1
Should this document be made available on the public website?	Yes. As part of Freedom of Information Publication Scheme
Is this document to be published in any other format?	No.

The Trust strives to ensure equality of opportunity for all, both as a major employer and as a provider of health care. This document has therefore been equality impact assessed to ensure fairness and consistency for all those covered by it, regardless of their individual differences, and the results are available on request.