Records Management and Information Lifecycle Policy (N-044)

Version Number:	3.2
Author (name & job title)	Lisa Davies, Head of Information Governance and Legal Services
Executive Lead (name & job title):	Hilary Gledhill, Director of Nursing
Name of approving body:	Information Governance Group
Date full policy approved:	September 2019 (v3.0)
Date Ratified at Trust Board:	September 2019
Next Full Review date:	September 2025

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	*IG Group - 21 September 2022*
Date EMT as approving body notified for information:	*September 2022*

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. INTRODUCTION

Records and Information Lifecycle Management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Records management policies form part of the Trust's Information Lifecycle Management together with other processes, such as records inventories, secure storage arrangements and records audit.

All NHS records are public records under the terms of the Public Records Act 1958. The Trust has a duty under the Public Records Act to make arrangements for the safe keeping and eventual disposal of all types of records.

Records are a valuable resource because of the information they contain. High quality information underpins the delivery of high quality evidence-based healthcare, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed. This is in line with the principles described within the Records Management Code of Practice for Health and Social Care 2021.

The Freedom of Information Act 2000 requires that an organisation can rapidly identify, locate or account for the disposal of records in relation to enquiries and requests for information that it receives. Both the Data Protection Act 2018 and the Freedom of Information Act 2000 require that organisations should have published and implemented policies and supporting procedures in relation to the creation, management and disposal of all types of records, regardless of the media on which they are held.

2. SCOPE

This policy relates to corporate information generated and received by the Trust in any format. Corporate information describes the records generated by the Trust's business activities, so will include records from the following areas:

- Estates
- Financial
- Information Management and Technology (IM&T)
- Human Resources
- Purchasing/Supplies
- Complaints

Issues specific to the management and use of clinical records can be found in the Health and Social Care Records Policy.

It is recognised that the Trust generates a huge amount of information in its day to day business and this will typically cover a wide spectrum of business critical documentation. For the purpose of this policy a distinction is made between a *record* and a *document*. A document becomes a record when it has been finalised and becomes part of the Trust's corporate information. At this point the record should not be amended and should be stored within the Trust's systems, usually on the Trust's V drive, in paper format, scanned or a combination of each. For example the minutes of a high level Trust committee will be first drawn up in draft format until they have been formally agreed and signed off at the next committee. They should then be retained in that form for the approved retention period.

It should be noted that access to the Trust's network, electronic systems and communications are logged and monitored. Logging activities includes but is not limited to monitoring system access to prevent attempts at unauthorized access, confirm access control systems are effective, or determine who has accessed a patient's record. The Trust recognises that Logs are records in

their own right and shall be kept as long as necessary or required for functional use or appropriate state regulation or law.

3. POLICY STATEMENT

The Trust is committed to safe keeping and safe disposal of records as required by:

- Public Records Act 1958
- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679
- Records Management Code of Practice 2021
- Standard Operating Procedure Data Protection Impact Assessments (SOP 16-005)

4. DUTIES AND RESPONSIBILITIES

Chief Executive
The chief executive has overall responsibility for records management in the Trust. As the accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate accurate information is available as required.

Senior Information Risk Owner
Designated member of staff with Board-level responsibility for records management supported by the deputy director of governance and patient experience.

Head of Information Governance and Legal Services and Data Protection Officer

- Responsible for the implementation of this policy.
- Undertake and maintain an inventory of all Trust records held in all formats.
- Establish a procedure for the closure of records when no longer current and effective disposal as soon as appropriate.
- Monitor performance by means of response times to subject access requests and Freedom of Information requests.
- Maintain a record of those records destroyed when they have reached the end of their administrative life.

Information Governance Committee
Monitor the Trust's activities in relation to this policy and to ensure compliance with law and guidance.

Caldicott Guardian
Responsible for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Heads of Department, Information Asset Owners, Chief Clinical Information Officers and Administrators

- Assist the head of information governance and legal services with the compiling of inventory of records for their particular spheres of responsibility.
- Update the Trust's Asset Register with any changes to the sets of records held within their sphere of responsibility.
- Ensure all new staff who create and retrieve records are familiar with this policy.

All Trust Staff

- Be aware of their personal responsibilities in respect of records keeping and records management as detailed in this policy.
- Be aware of responsibilities for any records that they create or use in the course of their duties in keeping with this policy.
- Be aware that any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.

5. PROCEDURES

Refer to Appendix 1 for procedures supporting this policy.

6. EQUALITY AND DIVERSITY

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust-approved EIA. No adverse impact was identified

7. IMPLEMENTATION

This policy will be disseminated by the method described in the Policy for the Development and Management of Procedural Documents.

The implementation of this policy requires no additional financial resource.

8. MONITORING AND AUDIT

The requirement for this policy is included in Standard 1 “The organisation has a record management policy including a records retention schedule” of the Data Security and Protection Toolkit. Trust performance against this standard is scored and submitted on an annual basis.

9. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

References/Evidence

Records Management Code of Practice - NHS Transformation Directorate

Glossary of Terms/Definitions

Appraisal
The process of evaluating Trust activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of government accountability and the expectations of researchers and other users of the records.

Corporate Records
These are records other than health records that are of, or relating to, the Trust’s business activities covering all the functions, processes, activities and transactions of the Trust and its employees.

It is important to make the distinction between a record and a document. In this context a document becomes a record when it has been finalised and becomes part of the Trust's corporate information.

Destruction
The process of elimination or deleting records beyond any possible reconstruction.

Disposal
The implementation of appraisal and review decisions. It could result in the destruction of the record, the transfer to an archive institution or the movement of records from one system to another, for example paper to electronic.

Health Record
A single record with a unique identifier containing information relating to the physical or mental health of a given patient who can be identified from that information and which has been recorded by, or on behalf of a health professional, in connection with the care of that patient.

Public Records Act 1958
For further information see the National Archives website at
http://www.nationalarchives.gov.uk/information-management/legislation/public-records-act/

Retention
The continuous storage and maintenance of records for as long as they are required by the Trust until their eventual disposal, according to their administrative, legal, financial and historical evaluation.

Tracking
Creating, capturing and maintaining information about the movement and use of records.

Appendix 1: Record Management Procedures

RECORDS MANAGEMENT PROCEDURES

1. CREATION

Each operational area (for example Finance, Estates, Human Resources) should have in place a process for documenting its activities in respect of records management. This should take into account the legislative and regulatory requirements within which the department operates.

Records creation is one of the most important processes in records management. However, creating a record is not enough unless the record is then filed into a filing system created and managed by the Trust. Whatever the format of the records, they should be saved into a proper records management system.

When creating a new record, a new set of records, or managing an existing set of records, the following must be considered:

- Referencing (see section 4)
- Version control standards (see section 7)
- Naming convention (see section 2)
- Where the original record should be filed

2. NAMING

Records should be easily retrievable from a system. It important that the department allocates a unique name to each record which is understood by all those who create new records into that set, or need to retrieve from it.

A meaningful name should be given which closely reflects the contents of the record with the most specific information at the beginning of the name, and the most general at the end. For example sets of records referring to named individuals will have the surname first followed by the first name (see section 4 for more guidance on this).

3. FILING STRUCTURE

A clear and logical filing structure that aids retrieval of records should be used.

Records should never be stored on the hard drive of a computer (C drive). Electronic documents should be stored in the departmental directory on the V drive.

The V drive has been structured to mirror the Trust structure, beginning at the highest Trust level, then down through directorates, departments and functions. Departments should arrange the file structure logically, for example by teams or functions. They should avoid a dense, multi-layered structure which requires drilling down through many levels to reach a particular document.

Staff should always ensure that access permissions within the V drive are set at the appropriate level for their department, so that only those staff who need to access a particular document are able to. Contact the IT Service Desk if you need assistance with this.

4. FILE/FOLDER REFERENCING

A referencing system should be used that meets the needs of that department and can easily be understood by staff members that create documents and records into that system.

Different types of referencing systems can be used but the main ones are explained below:

Alphabetical
Where the files are structured in alphabetical order within a subset, for example staff files by surname>>first name of the member of staff.

Numeric
Where a numbering system is used. The number may be generated by another system or sequentially. For example a log of requests generated may start at 001, 002 and so on, or suffixed with the year for example 2022-001, 2022-002.

Alphanumeric
A combination of both, so for example main subject heading (alphabetic) followed by a numeric; 1.1.1, 1.1.2 and so on.

If the date of a document is a key feature so that most recent is of relevance, for example storing email correspondence on the V drive it is useful to record the date in reverse followed by the name of the sender/recipient and a brief subject description, for example:

19 01 05 from P Smith Policies

This shows an email from P Smith about policies received on 5 January 2019.

When emails are being saved as documents on the V drive, select “Outlook Message Format” in the dialogue box “Save as type” otherwise any attachments within the email will not appear when the document is opened again.

5. NEW RECORDS MANAGEMENT FUNCTION

Under UK GDPR, organisations are required to conduct Data Protection Impact Assessments (DPIAs) where there is a new or change in use of personal data and a potentially high risk to privacy.

If there is a new records management function, then consideration will need to be given to the need to complete a DPIA. This will highlight potential risks to privacy and data protection, allowing actions to mitigate or eliminate that risk. This must be conducted prior to any processing being carried out. The DPIA SOP can be found at Data Protection Impact Assessment SOP

6. TRACKING AND TRACING

There should be system in place that controls the movement and location of files and documents through the system. Access to documents should be controlled and where files are moved around the Trust a simple system should be in place which identifies its location.

The system need not be complicated. A signing out book which staff complete when a record is removed, or a tracing card placed in the position of the original file can be used.

The book or the tracer card should include:

- name of file and/or file reference number where used
- the person who has possession of the file
- date when the file was sent or removed from the system
- name of the person within the department who has forwarded on the file.

Depending on circumstances, it may be prudent to include on the cover of the file, the person, department and address to which the file is to be returned when it is finished with.

If the file is required to be returned by a certain date, a task or reminder should be set up to prompt the department loaning the file to request its return.

Documents and files should always be transferred using the appropriate level of security. For guidance in this area consult:

- Safe Haven Policy
- Caldicott and Data Protection Policy
- Health and Social Care Records Policy
- Electronic Communications and Internet Acceptable Use Policy
- Code of Conduct for Employees in Respect of Confidentiality and Information Sharing

7. RETENTION AND DISPOSAL

When paper records are no longer required for business purposes, their placement in a designated secondary offsite storage area may be a more economical and efficient way to store them. Arrangements for offsite storage should take full account of the need to preserve important information and keep it confidential and secure.

Appraisal refers to the process of determining whether records are worthy of permanent preservation. This should be undertaken as part of the inventory process for each department (see section 8).

The retention schedules outlined in the Department of Health's *Records Management Code of Practice 2021* will be used for all sets of records. These minimum retention periods will be identified as part of the inventory process. The appraisal process will ensure that the records are examined at the appropriate time to determine whether or not they need to be retained for a longer period than is specified in the retention schedule. This decision will be made by a senior manager who has an appropriate understanding of the operational area to which the records relate, and in conjunction with the Information Asset Owner or Administrator if they are not the same person.

Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

The records inventory will identify the retention/disposal periods based on the retention schedule in the *Records Management Code of Practice 2021*. It should cover all records held by the Trust. Some common types of records with their minimum retention periods are listed in Appendix 2.

Disposal of non-active records at or before 20 years old should be done in conjunction with the Head of Information Governance and Legal Services and local places of deposit, this being the archivist departments at the Hull City Council and East Riding of Yorkshire Council, as required by the Public Records Act.

Records which have reached the end of their administrative life and not selected for archival preservation should be destroyed in a secure manner as appropriate to their level of confidentiality. Contractors, if used should be required to sign confidentiality undertakings and produce written certification as proof of destruction.

A record of destruction of records, showing reference, description and date of destruction should be maintained and preserved by the Information Asset Owner.

If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the Trust has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process completed. The cover of the record should be endorsed to make this clear.

8. VERSION CONTROL

It is recommended to use version control for business critical documents such as, but not restricted to, policies, strategies, business cases, project documents and high level reports. A Change Record Sheet should also be used where it is necessary to have a permanent record of what changes have been made to subsequent versions.

The method to be used is explained in the Policy for the Development and Management of Procedural Documents.

9. INVENTORY

The Information Governance Department will work with services to undertake an inventory of business critical documents included in the Scope of this policy. The inventory will be reviewed on an annual basis.

The inventory will establish the following:

- the records held within that department (title)
- the media on which they are held
- whether they are originals or duplicates
- brief description of the information held
- reason why this information is held
- whether documents contain personal data
- where the records are held
- retention period for the records
- action to be taken when the retention period is reached, e.g. transfer, disposal.

10. STORAGE

Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access and readable information.

When scanning documents, staff should ensure the quality of scanning by printing off the first few pages of scanned documents. This should be done the first time a scanner is used, when any changes are made to the settings or when a new type of document is scanned for the first time. A Scanned Images Tag Image File Format (TIFF) v6 or JPEG resolution of 150x150dpi is suitable for document archiving.

Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allows accessibility of the information corresponding to its frequency of use.

Information assets assessed as business critical should be included in Business Continuity Plans and should be risk assessed with mitigating actions in the case of an incident.

Appendix 2: Retention Periods for Records

RETENTION PERIODS FOR COMMONLY USED RECORDS

Please note, the following is a summary only. Consult the NHS Code of Practice for full guidance at
Records Management Code of Practice - NHS Transformation Directorate

TYPE OF RECORD	MINIMUM RETENTION PERIOD	DERIVATION	FINAL ACTION
Minutes of board meetings, committees, sub committees (master copies, including associated papers)	20 years	NHS code of Practice	Transfer to a Place of Deposit
Annual Report & Accounts	20 years	Care Quality Commission Recommendations	Transfer to a Place of Deposit
Audit Records (Clinical)	5 years from the date of completion of the audit	NHS code of Practice	Destroy under confidential conditions
Business plans, including local delivery plans	Life of organisation plus 6 years	NHS code of Practice	Destroy
Complaints	10 years from closure	NHS code of Practice	Destroy under confidential conditions
Data Input Forms (where the data/information has been input to a computer system)	2 years	Previous Guidance NHS code of Practice	Destroy under confidential conditions
Diaries (clinical)	2 years after the end of the calendar year to which they refer 8 years if containing clinical information	NHS code of Practice	Destroy under confidential conditions
Duty rosters	6 years after the date to which they relate	NHS Code of Practice	Destroy under confidential conditions
Electrical testing	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Freedom of Information requests	3 years after full disclosure:	NHS code of Practice	Destroy under confidential conditions
Fire Safety	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
General/Clinical Policies	30 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Health and Safety documentation	3 years	Previous guidance NHS code of Practice	Destroy under confidential conditions
Incident forms	Serious 20 years Not Serious – 10 years	NHS code of Practice	Destroy under confidential conditions
Incident occurrence notifiable to CQC	10 years	Care Quality Commission Recommendations	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	DERIVATION	FINAL ACTION
Litigation dossiers (complaints including accident/incident reports) Records/documents relating to inform of litigation	10 years from closure of case	NHS code of Practice	Destroy under confidential conditions
Logging information Server based system logs (eg Firewall, Advanced Threat Protection, VPN access) Application event and activities Logs (3rd party systems eg. SystmOne, Lorenzo, ESR, Oracle, PCMIS, IAPTUS etc) NHS Mail	Default is 180 days (where applicable, where it is less than this the rationale will be recorded in the system level security policy) From point of creation/modification for duration of the system	No national recommendation Default 180 days where applicable is in-line with NHS Digital NHS Mail: Data Retention Policy	
Maintenance of equipment	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Maintenance of premises	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Medical gas	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Money or valuables	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Patient Advice & Liaison Services (PALS) records	10 years after closure of the care	NHS code of Practice	Destroy under confidential conditions
Patient information leaflets	6 years after the leaflet has been superseded	NHS code of Practice	See Section 6 on permanent archive
Patients' property books/registers (property handed in for safekeeping)	2 years after the end of the year to which they relate	NHS code of Practice	Destroy under confidential conditions
Patient Surveys (Access to services etc)	2 years	Previous Guidance NHS code of Practice	Destroy under confidential conditions
Phone message books	2 years NB Any clinical information should be transferred to the patient health record	Previous Guidance NHS code of Practice	Destroy under confidential conditions
Press releases	6years	NHS code of Practice	See Section 6 on permanent archive
Project files (Major)	20 years	NHS code of Practice	See Section 6 on permanent archive
Project files (other)	6 years	NHS code of Practice	Destroy under confidential conditions
Public Consultations e.g. about future provision of services	5 years	NHS code of Practice	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	DERIVATION	FINAL ACTION
Purchasing of medical devices	11 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Purchasing (non-clinical)	18 months	Care Quality Commission Recommendations	Destroy under confidential conditions
Quality assurance records	12 years	NHS code of Practice	Destroy under confidential conditions
Records documenting the archiving, transfer to public records archive or destruction of records	30 years	Previous Guidance NHS code of Practice	See Section 6 on permanent archive
Requisitions	18 months		Destroy under confidential conditions
Research ethics committee records	5 years from date of decision	NHS code of Practice	See Section 6 on permanent archive
Risk Assessments (Non clinical)	8 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Staff employment	Until 70th birthday or 6 years after employment	Care Quality Commission Recommendations	Destroy under confidential conditions
Subject Access Requests (for access to records, other than Freedom of Information requests)	3 years after closure	NHS code of Practice	Destroy under confidential conditions
Timesheets (relating to a Group or Department, e.g. Ward where the timesheets are kept as a tool to manage resources, staffing levels)	6 months	Previous Guidance NHS Code of Practice	Destroy under confidential conditions
Use of restraint or deprivation of liberty	Life of the medical record	Care Quality Commission Recommendations	Destroy under confidential conditions
Water safety	3 years	Care Quality Commission Recommendations	Destroy under confidential conditions
Website and Intranet	6 years	NHS Code of Practice	Review and consider transfer to a Place of Deposit
Audio recorded telephony systems	3 years	NHS Code of Practice NHS Resolution	Review and if no longer needed destroy under confidential conditions
GP temporary resident forms	2 years after treatment	NHS Code of Practice	Copy sent to responsible GP for inclusion in the primary care records. Then review and if no longer needed destroy under confidential conditions

Please note there is currently a restriction on destroying any record which may be relevant to the following public Inquires:

- The Infected Blood Inquiry
- The Independent Inquiry into Child Sexual Abuse (also known as the Goddard Inquiry)
- The UK Covid-19 Inquiry

Appendix 3: Equality Impact Assessment (EIA) Toolkit

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: Records Management and Information Lifecycle Policy
2. EIA Reviewer (name, job title, base and contact details): Lisa Davies, Head of Information Governance & Legal Services, Mary Seacole Building, 01482 477840
3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? Policy

Main Aims of the Document, Process or Service
The Records Management and Information Lifecycle Policy aims to set out how the Trust manages its non-clinical information from creation of a record through to its archiving or destruction.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender Reassignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	Low	Internet search. Evidence from Care Quality Commission Patient Survey results. Evidence from issues dealt with by PALS and Complaints Department. The policy will follow the Trust's policies for communicating with service users who are unable to understand English, are non-literate or lack capacity. Scrutiny of Information Governance issues log and quarterly reports to the Information Governance Committee. Secure storage, processing and destruction of sensitive, confidential information is covered in Trust Safe Haven and Data Protection Policies.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental Health (including cancer, HIV, multiple sclerosis)	Low	As above

Sex	Men/Male Women/Female	Low	As above
Marriage/Civil Partnership		Low	As above
Pregnancy/ Maternity		Low	As above
Race	Colour Nationality Ethnic/national origins	Low	As above
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	As above
Sexual Orientation	Lesbian Gay Men Bisexual	Low	As above
Gender Reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	As above

Summary

Please describe the main points/actions arising from your assessment that supports your decision above: There was no evidence of potential negative effect from a search of the internet, any relevant information from the Care Quality Commission Patient Survey results or results from issues dealt with by PALS and Complaints Department. Any equality issues in respect of this policy would be captured through the Trust's PALS and Complaints processes, or reporting as adverse incidents, safeguarding and so on.	
EIA Reviewer: Lisa Davies	
Date completed: September 2022	**Signature:** Lisa Davies

Appendix 4: Document Control Sheet

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Policy		
Document Purpose	This policy relates to corporate information generated and received by the Trust in any format. Corporate information describes the records generated by the Trust's business activities, so will include records from the following areas: • Estates • Financial • Information Management and Technology (IM&T) • Human Resources • Purchasing/Supplies • Complaints		
Consultation/ Peer Review:	Date:	Group / Individual	
List in right hand columns consultation groups and dates		Information Governance Group	
Approving Committee:	Information Governance Group	Date of Approval:	18 August 2019
Ratified at:	Board	Date of Ratification:	10 September 2019
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*	None	Financial Resource Impact	None
Equality Impact Assessment undertaken?	Yes [ ]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [✓]
Master version held by:	Author [ ]	HealthAssure [✓]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	• All staff email as part of the Midweek Global with a link to the policy.		
Monitoring and Compliance:	Compliance of this policy is monitored within the Data Security and Protection Toolkit.		

Document Change History:			
Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
2.00	*Review*	*Feb 2012*	*The Outcome 21: Records of the Care Quality Commission - describe a number of records and the minimum retention period, now included in Appendix B.* *Changes to job titles and roles. The role of the Information Asset Owner (IAO) has been established and is key to implementing and monitoring compliance of this policy.* *An IG Toolkit Audit, undertaken at the end of 2011 identified a requirement in standard 9-601, for procedural guidance on the management of non-clinical records. The policy now includes specific practical guidance in Appendix A.* *http://www.cqc.org.uk/sites/default/files/media/documents/essential_standards_of_quality_and_safety_march_2010_final_0.pdf*
2.1	*Review – minor amends*	*Nov 2016*	*Minor changes to reflect job titles.* *The code of practice has been updated and is now the Records Management Code of Practice for Health and Social Care 2016* *Retention periods in Appendix B changed to reflect new Code of Practice*

2.2	*Review – minor amends*	*Sept 2018*	*Update references to Data Protection Act 2018 and General Data Protection Regulation.*
3.0	*Review*	*Sept 2019*	*Change of title from Head of Corporate Governance to Head of Information Governance and Legal Services.* *Inclusion of Retention Periods for Trust's Website and Intranet, Audio recorded telephony systems and GP temporary resident forms.* *Inclusion of the destruction restrictions imposed by the Goddard Inquiry and the Infected Blood Inquiry.*
3.1	*Review – minor amends*	*June 2021*	*Added section on Logging information to Section 2.* *Log retention information added to the table at Appendix 2*
3.2	*Review – minor amends*	*Sept 2022*	*Updated roles* *Inclusion of DPIA* *Update to Health's Records Management Code of Practice for Health and Social Care 2021* *Inclusion of UK Covid 19 Inquiry* *Approved at IG Group -*