NHS
Lincolnshire Community
Health Services
NHS Trust

Records Management Policy

(Clinical and Corporate Records, Access to Information, Scanning Documents)

Reference No:	P_IG_28
Version:	2
Ratified by:	LCHS Trust Board
Date ratified:	11 May 2021
Name of author:	Data Protection Officer
Name of responsible committee:	Information Governance Management Assurance Group
Date approved by responsible committee:	21 April 2021
Date issued:	May 2021
Review date:	May 2023
Target audience:	All staff and third-party contractors employed by LCHS
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Version Control Sheet

Version	Section/Para /Appendix)	Version/Description of Amendments	Date	Author/ Amended by
1		Amalgamation of policies (P_IG_04, 11, 19, 20), content previously ratified and further content updated to reflect GDPR.	June 2018	Kaz Scott
2		Full Review UK GDPR	Feb 2021	Kaz Lindfield-Scott
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Contents

Lincolnshire Community Health Services NHS Trust

Records Management Policy

Policy Statement

Background

The Trust has a duty under the Public Records Act to plan for the safekeeping and eventual disposal in accordance with the schedule. This includes records controlled under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of their format. The Act requires all public bodies to have effective systems to deliver their functions.

Records also serve the wider purposes of teaching, research and clinical audit as well as providing evidence in the event of litigation. They are a vital source of statistical and managerial information for the day to day running and future planning of the NHS.

This policy relates to all operational records held by the Trust and pulls together the arrangements covered by the following policies:

- Consent to Treatment Policy
- Data Protection Policy
- Safeguarding Children Policy
- Inter-Agency Information Sharing Protocol
- Risk Management Strategy
- Incident Reporting Policy
- Information Security Policy
- Information Risk Policy

The policy is split into sections and details specific procedures for achievement of the policy standards.

Statement

Staff working for the Trust will ensure that they comply with the requirements of the Data Protection (DP) Legislation, which brings together the UK General Data Protection Regulation (GDPR) & DP Act 2018.

Responsibilities

All staff have a responsibility for maintaining confidentiality and handling information appropriately.

Training

All staff are responsible for their own record keeping and must maintain an up to date awareness of legal and ethical issues concerning the subject.

Dissemination

The policy will be published on the Trust website.

RECORDS

The Trust manages all aspects of records whether internally or externally generated and in any format or media type, from their creation to their eventual disposal.

The Trust requires records to:

- Support patient care and continuity of care;
- Support improvements in clinical effectiveness through research;
- Assist clinical and other record audits;
- Protect the interests and rights of patients and employees

All records created and maintained by the Trust are Public Records under the Public Records Act 1958 and 1967 and the Trust must ensure policies and procedures are in accordance with the following statutory and NHS guidelines.

- Data Protection Legislation (DP)
- Freedom of Information Act 2000
- NHS Code of Practice for Confidentiality
- The Code: Professional standards of practice and behaviour for nurses and midwives
- NHS Resolution Risk Management Standards
- Data Security and Protection Toolkit (DSPT)

The Records Management Code of Practice 2020 has been published as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

The Trust is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from doing so.

Scope and Definitions

A record is anything which contains information, digital or paper based – in any media - which has been created or gathered as a result of the work of NHS employees, including:

- Clinical or Corporate records (Digital or Paper)
- Audio, photographs, scans
- Emails

All staff employed within the Trust (including those on temporary contracts, students or Bank/Agency staff) who are involved in handling, contributing to or creating records, making them aware of their responsibilities to meet the requirements and standards relating to the records.

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs and preserving an appropriate historical record.

The key components of records management are:

- Create, Use, Retain, Appraise, Destroy

The term **'Records Life Cycle'** describes the life of a record from its creation and finally either confidential disposal or archival preservation.

Accountability – adequate records are maintained to account fully and transparently for all actions and decisions, in particular:

- To protect legal and data subject rights of staff or those affected by those actions
- To facilitate audit or examination
- To provide credible authoritative evidence

Quality – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed.

Accessibility – that records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the Trust.

Security – that records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled. Audit trails will track all use and changes.

Duties and Responsibilities

The Trust Board is ultimately responsible for ensuring that Records Management function is addressed

Chief Executive

Has overall accountability for Records Management within the Trust as the Accountable Officer; the role provides assurance, through a Statement of Internal Controls, that all risks to the organisation, including those relating to the management of records are effective and mitigated.

Caldicott Guardian

Is the Medical Director; this is an advisory role and has responsibility for protecting the confidentiality of information and ensuring it is shared appropriately and securely. The Caldicott Guardian is supported by the Data Protection Officer.

Senior Information Rick Owner

An Executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

Data Protection Officer

Operational responsibility for the Records Management Policy and is responsible for the overall development and maintenance of the Records Management policy and for ensuring it complies with legal and regulatory edicts. They are also responsible for providing learning and development with key learning points and for monitoring compliance to assess its overall effectiveness as will also give advice and guidance to inform staff of their obligations.

Heads of Service

Responsible for records and information created by their staff. Heads of Service are also responsible as Information Asset Owners (IAO). An IAO is obliged to enforce policies and procedures locally relating to information management and give assurances to the SIRO that they are being met. This includes an annual audit of information assets, removable media and data flow mapping.

Managers

Responsible for ensuring that staff under their direction and control are aware of the policies and procedures and for checking that those staff understand and appropriately apply the policies in carrying out their day to day work.

All staff
Responsible for ensuring they comply with this policy and local guidance where this exists. Staff are also directed by their professional codes of practice which may also include guidance on record keeping. Staff must report all incidents involving records via the incident reporting system. This includes the loss of or missing records.

Information Governance Management Assurance Group (IGMAG)
Will approve guidance and procedures related to records management. This is the sub-group with delegated duties to deal with information governance and overall records management issues and reports to the Finance, Performance and Investment Committee (FPIC).

The Trust is subject to a number of legal, statutory and good practice guidance requirements covering records.

All staff members, volunteers and persons acting on behalf of the Trust

- All employees have a responsibility for any records they create or use. Any records created by an NHS employee are public records and may be subject to both legal and professional obligations.
- Staff must attend relevant training covering records management.
- Staff must refer any concerns and incidents to their manager.
- This responsibility will be set out in all job descriptions.

Training
All managers and staff responsible for records will receive training covering records management at least annually. This may be delivered through e-Learning or Face-to-Face Training.

To comply with legislation, this training will follow the HORUS principles:

- **H**olding information securely and confidentially;
- **O**btaining information fairly and efficiently;
- **R**ecording information accurately and reliably;
- **U**sing information effectively and ethically;
- **S**haring information appropriately and lawfully

Management of Records
Records are created so that information is available within the Trust to:

- Deliver the services offered by the Trust to the community.
- Ensure records are kept for the operation of the business and are correctly managed.
- Support day to day business to support decision making, delivery and continuity of care.
- Support evidence-based practice, research, medical and other audits.
- Meet legal requirements, including requests from data subjects under DP legislation.
- Assist the Trust in defending any legal claims against it or its staff.
- Clinical entries should be recorded within 24 hours to support continuity of care.

The following is considered unacceptable practice;

- Delete or erase notes, such that the entry is no longer legible.
- Use “white out” correction fluids in any part of a paper record.
- Change original entries or made by another person unless there is a legal requirement.
- Amend the record of an opinion or judgement recorded by a healthcare professional, whether accurate or not, because the recorded opinion or judgement is essential for understanding the clinical decisions that were made and to audit the quality of care.

Naming Folders, Files and Documents

Naming conventions are standard rules to be used for naming both documents and electronic folders. Corporate standards must be followed in the naming of files and folders. It is unacceptable for any documents to leave the Trust without it showing the Trust as being the owner of such documents.

Version Numbers

Where the record is likely to be replaced in the future by a new version, e.g. a policy, a version number should be included, both in the filename and also the document itself,

Structuring Folders and Files

A well thought out structure of folders (also known as directories or classification schemes) for filing documents is a key element to efficient electronic record keeping. Folder titles should be clear and concise and adequately describe the contents.

Access to folders can be set up with varying degrees of permissions / controls, depending on the nature of the contents and who requires access.

Where to Save Documents

There are generally main areas where documents can be saved – either shared secured or personal folders. These are located on the network.

Storage of records

All records must be kept secure in their workplace. All record storage systems must have an effective tracking system in the form of a records inventory which will aid easy retrieval should the record be required if stored offsite.

Transportation of Physical Records

It is recognised that records, both electronic and paper based, should not be taken off Trust premises. However, it is acknowledged that there are operational reasons for doing so. These include transporting records between premises via the internal courier service, or for clinicians with an operational need to take the records between sites personally.

Only such notes as are necessary for those purposes may be taken, and they must remain with the individual at all times. If there is a need to transport clinical records staff are to ensure the process is as safe as possible.

Leaving records in an unattended private vehicle would require a justifiable reason. Where such justification is thought to exist, the records must be out of sight, for instance in the boot, and the vehicle locked.

Sending Records by Post

This section applies to internal post, external post such as the Royal Mail and any other postal or courier / delivery service.

All records relating to vulnerable, children in need, looked after or child protection plan must be sent via the Child Health Department and must have been seen by the Designated / Named Nurse for Child Protection before leaving the Trust. They must contain a transfer out summary and be sent by special delivery to the Child Health Department of a receiving NHS organisation.

There is also the option to scan and send securely by e-mail using an approved secure e-mail or the encryption available.

Corporate records relating to commercially sensitive must be in appropriately addressed in a secure, sealed envelope or sent electronically by secure e-mail or encryption.

Electronic Transmission of Personal Data

Computers with access to personal data, whether standalone or networked, must have security measures in place to prevent unauthorised access. Regular audits will be conducted to ensure compliance. Action will be taken against staff that have accessed information that they do not have a legitimate business requirement.

Retention, Archiving and Disposal Procedure for Records

There is a strict process for the retention and disposal of records to ensure compliance with legal obligations, operational, research and safety reasons. In addition to this, the process allows the Trust to effectively manage the storage space available.

If the records are no longer active, these will either be securely stored onsite or transferred to off-site storage or disposed of in line with the records retention schedule. For all records the archive year is the calendar year in which the last entry was made. The destruction date is the appropriate number of years pertaining to the relevant type of record,

Records that require regular and easy access can be retained on site in individual Directorates and must be secured in a lockable filing cabinet or a secure cupboard/records room. The storage of paper records should be discouraged, and the use of electronic recording is encouraged.

Retention of Records

All records are retained for a minimum period of time for legal, operational, research and safety reasons and will depend on the type of record. A record can only be destroyed when it fulfils the following criteria

- last contact with the Trust is over the minimum period for that type of record
- Method of destruction and certificate (where applicable) unless under contract

Permanent Preservation

Records which seem likely to provide material for research or have historical value should be scrutinised with a view to transfer to an 'Approved Place of Deposit' located at the Lincolnshire Archives, St Rumbold Street, Lincoln. LN2 5AB.

Destruction and Disposal

All confidential waste must be placed in the allocated "Shred-it" consoles where this applies or shredded. The equipment must be a Crosscut or Confetti-Cut Shredder with a minimum Din level 3. Confidential shredded waste can go out with normal recycling and non-confidential waste placed in the cardboard recycle bins.

Where records are destroyed by an approved contractor a destruction certificates should be retained to provide legal proof of destruction in case the records are subsequently requested under a 'right of access' or litigation purposes. This could be paper or electronic destruction as part of a contract exit strategy.

Missing Record Procedure

When records are mislaid or missing this may be due to;

- Record with Medical Secretary or staff unable to retrieve the record
- Record not tracked or misfiled or patient unable to locate patient-held record
- Majority of records are electronic, therefore misplaced/misplaced records is decreased

When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of all actions taken.

Sharing Information

All staff should work towards rationalising record collections through sharing appropriately ensuring it meets legal and statutory obligations.

Important points:

- Data belong to the Trust and not to individuals or departments
- NHS records are public records
- The Trust recognises that there are restrictions on the disclosure of information

Confidentiality and Security of Records

The storage, distribution, use and disposal of records will conform to relevant legislation e.g. Data Protection Act 2018, Freedom of Information Act 2000 and ISO 27001:13 – Information Security, and NHS guidance such as, Caldicott Principles, NHS Code of Practice on Confidentiality 2003, and local policies, taking into account best practice.

Records Audit

An Audit will be undertaken annually and will consist of an audit of electronic records to promote a paper-light / paperless environment.

In accordance with requirements within the NHS Resolution (NHSR) and the Care Quality Commission (CQC), the Trust is required to review record keeping standards annually.

The audit will:

These may include; Privacy Officer Alerts, Investigations, Complaints, Disciplinary, Access Controls amongst a few. These findings are reported to IGMAG.

- Identify areas of operation and identify which procedures and/or guidance should comply
- Follow a mechanism to cover any gaps if these are critical to the creation and use of records and use a subsidiary development plan.
- Set and maintain standards by implementing new procedures, including obtaining feedback where non-conformance to the procedures is occurring and recommend a tightening of controls and adjustment to related procedures.

Clinical Diaries

The use of clinical paper diaries is prohibited due to the risk of loss. Any staff member found to be in breach, may be subject to disciplinary procedures. Mobile working is available to access systems offline or mobile apps whilst working in the community.

Monitoring

Incidents relating to records will be monitored through the Incident Reporting Policy. Serious incidents i.e. loss of records, misidentification, breaches of confidentially, failure to comply with DP legislation will be subject to further investigation which may include a Root Cause Analysis investigation. All Serious Incidents Requiring Investigation (SIRI) which meet the screening criteria through the Data Security and Protection Toolkit (DSPT) will follow that process.

DATA SUBJECT ACCESS REQUESTS (DSARs)

This gives direction to staff about the provision on the Rights of Access under UK-GDPR for data subjects and their representatives to make a request for personal data processed by the Trust and also applies to entries made by health professionals in records for integrated services.

The main legislative measures that give rights of access to health records include:

- **Data Protection Legislation** – rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf.
- **The Access to Health Records Act 1990** – right of access to deceased health records by specified persons.
- **The Access to Medical Reports Act 1988 –** right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes

UK legislation sets out the principles concerning personal data. The Trust will always strive to ensure that personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:
"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Duty of Confidence

All those working for or with the Trust, who record, handle, store or otherwise have access to personal data have a common-law duty of confidence. All employees have a duty to maintain professional ethical standards of confidentiality.

Any information, given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else.

There will be cases where information may need to be shared with a third party, even when consent by the person or their representative has been refused or where a person does not have capacity to consent. Where requests for information are received by the Trust, they should always be considered on a case by case basis.

Data Protection and Compliance
All staff are reminded that all requests for information made under UK legislation must be handled by the Data Protection and Compliance Team unless otherwise advised by the DPO.

Access

- A Data Subject has a right to apply for access to their records. Requests are not required to be in writing. Where a person seeks access to their own record, the Trust should ensure that sufficient identity checks are undertaken to be satisfied the person is entitled to the records. These circumstances include:
- Where the release of information could cause mental or physical harm
- Where access would disclose information relating to or provided by a third party who has not consented to that disclosure.

Access by a Representative
If a request is received from a representative (provided the person has capacity) the person is the only one allowed to authorise the release of their record. The representative may include any person the individual consents to have access to their record but not limited to;

- Persons relative, a friend or Litigation friend
- Solicitor or another legal representative

If a person is unable to authorise the release due to a lack of mental capacity, then a person who has been legally appointed to act on their behalf has the right to apply.

This may include:

- A person holding a Lasting Power of Attorney (LPA) for Health and Welfare
- A person holding an Enduring Power of Attorney (EPA) if before Oct 2007
- An independent Mental Capacity Advocate (IMCA)

Where a request is received from a legally appointed representative, they should be asked to produce evidence that they hold an LPA be registered with the Office of the Public Guardian.

There may be occasions where a representative (such as a family member) who does not have an automatic right of access to the record, seeks disclosure. There is no right for next of kin to review the records of an incapacitated patient, there may be circumstances where it is appropriate. Requests of this nature must always be considered on a case by case basis.

The Court of Protection can also appoint deputies for this purpose. This may entail giving access to relevant parts of a record unless the professional can demonstrate this would not be in the best interests.

Access to Records by other Agencies
There will be occasions for requests for access to patient records from other Agencies. These may include the Coroner, Police, General Medical Council, Social Services and other NHS organisations.

The Trust will consider carefully when information can be shared with other agencies and whether consent can and should be taken beforehand. The Trust will consider requests carefully and on a case by case basis.

Access Records of a Deceased Person
This is governed by the Access to Health Records Act (1990). Under this legislation their Personal Representative, Executor, Administrator or anyone having claim resulting from the death has the right to apply for access.

Individuals have a legal right of access under the Act only where they can establish a claim arising from a death.

If a requestor wishes to make a complaint these must be directed to the DPO to handle in the first instance. If the complaint cannot be resolved the requestor must be directed to the Information Commissioners Office.

The UK GDPR only applies to information which relates to an identifiable living individual. Information relating to a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

When Police approach staff for information
When a Police Officer makes a request for information of a Data Subject, this must first be validated by the Data Protection and Compliance Team (DP&C) and disclosed under the following circumstances:

- With the appropriate consent of the person has been received
- Where the consent has been received from the police and signed by the Authorising Officer who must be ranked Police Inspector or higher. For other 'relevant bodies' a Senior Manager.

- This may be for;

a. Police and Criminal Evidence Act 1984 – Sections 19 & 20.
b. Terrorism Act – Sections 19 & 39.
c. Fraud Act 2006 – Section 1
d. Computer Misuse Act – Section 1 now the Police and Justice Act 2006 section 35
e. Serious Crime Act 2007 – Section 68 & 72
f. Exceptional circumstances as defined by the DP&C Team; information can be released.

There may changes in respect EU Legislation and UK Law and no further changes have been made available which affect the above.

Other occasions where the Trust may be able to release without consent are;

- Whether there is a threat to public health and safety or a risk of death / serious harm to the person or other individuals
- The circumstances of the matter under investigation; or any order of a Court
- If the public interest in the specific circumstances outweighs the individual's right to privacy e.g. in 'distress' cases i.e. reported missing person

For the above points guidance must be sought from the DPO.

Response Targets
The UK legislation requires the Trust to complete all request within one calendar month and in exceptional circumstances if it is not possible this can be extended to a further two months under advice from the DPO and the applicant must be informed.

SCANNING DOCUMENTS

Legal Admissibility (LA) is a core Records Management principle and if a document is scanned and it must be a true representation of the original.

The Trust has a duty to ensure documents created or scanned, stored and migrated through electronic systems meet the evidential weight as outlined in the Civil Evidence Act 1995 to ensure BS 10008 LA should a Court require it

Compliance within it does not guarantee LA. It is possible to maximise the evidential weight of a record/document by setting up authorised procedures and being able to demonstrate in court that those procedures have been followed.

Procedures are defined which need to be implemented in order to comply. To demonstrate that it complies with the five principles of information management.

They are:

- Recognise and understand all types of information
- Understand the legal issues and execute 'duty of care' responsibilities
- Identify and specify business processes and procedures
- Identify enabling technologies to support business processes and procedures
- Monitor and audit business processes and procedures

Statement

This is applicable to any Trust system that stores information electronically and its outputs. It covers aspects of the information management processes that affect the use of information in normal business transactions.

This is to establish guidelines for:

- Authenticity and Integrity of stored data
- Scanned, stored and electronically communicated data

The purpose is to:

- Provide guidance on process, procedure, audit in order to ensure authenticity, integrity, security and LA of scanned, stored or migrated information
- Improve reliability of, and confidence in, communicated information, and electronic documents to which an electronic identity is applied
- Maximize the evidential weight which a court or other body may present information
- Provide confidence in inter-organisation information sharing
- Provide confidence to external inspectors (i.e. regulators and auditors) that the Trust's information and business practices are robust and reliable

The requirement to authenticate electronic documents that have evidential significance to a Trust may be vital to continued operations.

Information security is key when discussing LA issues and is the authenticity of the stored information in the form of robust audit trails that evidence;

- When the electronic information was captured, was the process secure?
- Was the correct information captured complete and accurate?
- During storage, was the information changed, either accidentally or maliciously?
- What is the process for scanning paper originals into the system? Can the Trust evidence the quality and integrity of the original document has been maintained?
- Information security implementation and monitoring are key to demonstrating authenticity.

It is essential at the planning stage to consult with appropriate third parties who will need to use, inspect or have a material interest in the results from authenticated systems. Examples of such third parties are:

- Receiving Parties, Auditors, Legal Experts, Technical and Operational Staff and The Courts

The Trust should be aware of the value of its electronic identity management systems and execute its responsibilities to those systems under the duty of care principle.

To fulfil its duty of care obligations, the Trust should:

- Be aware of and demonstrably comply with legislation and regulatory bodies
- Establish a chain of accountability and assign responsibility for all relevant activity
- Keep abreast of developments with the appropriate bodies and organisations

Training
Training needs of staff will vary according to the local scanning processes and procedures constructed to underpin local service needs.

Process
This applies to information scanned and electronically stored within an Information System and will provide guidance to ensure authenticity, integrity and availability.

The purpose of the process is to ensure:

- Authenticity, Integrity and Availability of stored data
- LA of scanned, stored and electronically communicated data
- Improve reliability and confidence in communication in electronic documents.
- Provide confidence in inter-organisation information sharing

Type of Document
Identify documents for scanning. Check for ultra-shiny paper - this will not scan properly and needs to be photocopied before being scanned.

Duplication
If duplications are found these should be destroyed and not form part of the scanned document. Any handwritten information that has been added after the date of the original document should be retained and scanned.

Misfiling
Check that all the information in the document pertains to the same person (NHS No: Name and DoB), Employee or appropriate service department. If misfiled information is found it must be relocated to the appropriate record.

Quality of Original or Photocopy
If the original document is of poor quality, it is unreadable and photocopying and/or enhancing does not improve the readability, a note should be placed on file stating **‘Parts of this document were unable to be scanned due to the poor image quality of the original’.**

Images
Image processing is a post scanning technique to improve the quality of a scanned document. There may be good reasons for improving image quality, but it is <u>**NOT**</u> permitted for clinical photography in case essential detail is removed.

Images may be stored as a JPEG or Bitmap, TIF or GIF but storing as a file is recommended as it will help to retain the integrity of the image. This will also depend on the file formats which are accepted as part of the system.

Quality Control
It is important to be able to demonstrate to a court that the quality controls are adequate, and a check should be made of the paper document against the scanned document, ensuring that: -

- The same number of pages has been scanned, pages are legible and exact replicas

Retention
Original documents should not be destroyed until quality checks have taken place and assurance the scanned documents are legible and stored securely.

Audit
The audit trail as a minimum will log details of each significant event in the life of the document within the system. The audit will be generated by the system with details of the user, date and time and actions or any smartcard details of the system uses them for access control.

Security and Protection
This covers user access and support any audits or investigations.

Document Deletion
It may be necessary to amend or delete documents or parts of documents which will be identified via the system audit trail or to meet legal requirements when no longer required.

NHSR Monitoring

Minimum requirement to be monitored	**Process for monitoring e.g. audit**	**Responsible individuals/ group/ committee**	**Frequency of monitoring /audit**	**Responsible individuals/ group/ committee (multidisciplinary) for review of results**	**Responsible individuals/ group/ committee for development of action plan**	**Responsible individuals/ group/ committee for monitoring of action plan**
DSPT Standards	Review / Audit / Reports	DPO	Annual	DPO / IGMAG	DPO / IGMAG	DPO / IGMAG

Equality Impact Analysis Screening Form

Title of activity	Records Management Policy		
Date form completed	Mar 2021	Name of lead for this activity	Kaz Lindfield-Scott

Analysis undertaken by:		
Name(s)	Job role	Department
Kaz Lindfield-Scott	Data Protection Officer	Data Protection and Compliance

What is the aim or objective of this activity?	To provide effective management and accountability governance structures, processes, policies and procedures and a comprehensive IG/DP training adequately resourced to manage and embed IG and DP throughout the Trust.
Who will this activity impact on? *E.g. staff, patients, carers, visitors etc.*	All Staff and Service Users

Potential impacts on different equality groups:

Equality Group	Potential for **positive** impact	**Neutral** Impact	Potential for **negative** impact	Please provide details of how you believe there is a potential positive, negative or neutral impact (and what evidence you have gathered)
Age	☐	☒	☐	
Disability	☐	☒	☐	
Gender reassignment	☐	☒	☐	
Marriage & civil partnerships	☐	☒	☐	
Pregnancy & maternity	☐	☒	☐	
Race	☐	☒	☐	
Religion or belief	☐	☒	☐	
Sex	☐	☒	☐	
Sexual Orientation	☐	☒	☐	
Additional Impacts	☐	☒	☐	

If you have ticked one of the above equality groups please complete the following:

Level of impact

	Yes	No
Could this impact be considered direct or indirect discrimination?	☐	☒
If yes, how will you address this?		

	High	Medium	Low
What level do you consider the potential negative impact would be?	☐	☐	☐

If the negative impact is high, a full equality impact analysis will be required.

Action Plan

How could you minimise or remove any negative impacts identified, even if this is rated low?
How will you monitor this impact or planned actions?
Future review date: