Humber Teaching
NHS Foundation Trust

STANDARD OPERATING PROCEDURE

SCANNING OF PHYSICAL DOCUMENTATION

Document Reference	SOP19-007
Version Number	2.0
Author/Lead **Job Title**	Lisa Davies, Head of Information Governance and Legal Services Karen Robinson, Information Governance Officer
Instigated by: **Date Instigated:**	Information Governance Group 2018
Date Last Reviewed:	November 2021
Date of Next Review:	November 2024
Consultation:	If a clinical SOP include lead clinician and relevant clinical network If a general SOP include all affected team leaders Include when and how consultation took place
Ratified and Quality Checked by: **Date Ratified:**	Information Governance Group 17 November 2021
Name of Trust Strategy/Policy/Guidelines this SOP refers to:	• Health and Social Care Records Policy • Records Management and Information Lifecycle Policy

VALIDITY – All local SOPS should be accessed via the Trust intranet

CHANGE RECORD

Version	Date	Change details
V1.0	Sept-18	New SOP
V2.0	Nov-21	Major changes to document • Minor changes to job titles and references. • Additional clarification that letters approved within the clinical system do not need to be scanned once signed. Removed the requirement to add the date of scanning and the name of the staff member scanning and detailed that this is captured within audit data. Included the requirement that Lloyd George envelopes must not be destroyed. Approved Information Governance Group 17-Nov-21

Contents

1 Introduction

Humber Teaching NHS Foundation Trust is moving towards a society in which the use of paper is significantly reduced in favour of a more digital way of working. In order for this to be achieved the Trust acknowledges that the scanning of physical documents will greatly increase and become part of the Records Management process.

This procedure sets out the necessary guidelines to assist all employees on the responsibilities and practices in place, in relation to the scanning process.

The scanning of physical documents raises questions relating to the disposal of original papers and the legal admissibility of an electronic image. At present there is no definitive law regarding the legal admissibility of scanned documents over paper originals. Certain guidelines have been developed to aid the ever-growing number of government departments, public authorities and private companies that are working towards a more digital future.

This procedure adheres to the guidelines set out in BIP 0008:2008 to the British Standard on legal admissibility and evidential weight on scanned records. This code of practice provides guidance on the use of electronic images as evidence in legal situations.

2 Scope

This procedure applies to all employees of the Trust, including all staff who are seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid an honorarium.

This procedure applies to all information handled by staff when scanning into a digital format. Any physical filing that is transferred onto an electronic system must follow this policy according to the procedures set out.

This procedure will apply to any persons that have access to paper documents belonging to the Trust, and considers scanning to be the most constructive way forward when working in a paper light environment. This procedure applies to patient and corporate records.

3 Duties and Responsibilities

Chief Executive

The Chief Executive has overall accountability and responsibility for Records Management within the Trust.

Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of personal confidential data. They are responsible for ensuring personal confidential data is shared in an appropriate and secure manner.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner (SIRO) has overall ownership of the organisation's information risk and acts as champion for information risk within the Trust. The SIRO is responsible for the on-going development and day-to-day management of the Trust's Risk Management Programme for information privacy and security.

Head of Information Governance, Legal Services and Data Protection Officer
Will have overall operational responsibility for the management of the Medical Records Service and ensure that the procedure is implemented Trust-wide. They will also support the Executive Directors in the investigation of reported adverse events related to medical records and breaches in standards specified in this procedure and ensure that any lessons learnt are implemented to improve practice and standards.

Directors and Heads of Service
All Directors and Heads of Service are personally accountable for the quality of records management within the Trust, and all line managers must ensure that their staff whether administrative or clinical are adequately trained and apply the appropriate guidelines. Staff must have an up-to-date knowledge of the laws and guidelines concerning confidentiality, data protection and access to health records.

Chief Information Officer
The Chief Information Officer is responsible for ensuring that our organisation become paperless and uses a digital by default approach. The Digital Delivery Group is responsible for compliances to this procedure.

All Staff
All staff are responsible for ensuring that the information scanned is in line with the guidance of this procedure. Staff must help to achieve the paperless strategy by using less paper documents and implementing more electronic methods where possible.

4 Procedures

4.1 What to scan
Any physical documentation that would be deemed necessary and/or noteworthy to a patient's health and well-being or treatment, will need to be scanned. If the physical item is essential information that would be stored on a physical file, this must be scanned into the relevant system. Any documents that can be created electronically in the first instance must be completed online and not duplicated in a physical document and scanned.

Any physical documentation that does not belong to the Trust must be kept in its original format and not scanned. This can include deeds, guarantees, or certificates which are not the property of the Trust. These can only be scanned and destroyed with written consent from the owner.

Do not scan any duplicate documents that are already on a system used by staff. This includes letters generated and approved within the clinical system that are now signed. Once a document is scanned it should not be re-printed with the exception of outside agencies (If no electronic transfer method is available) or a subject access request.

In line with the Health and Social Care Records Policy, the Information Governance Group will identify and recommend the destruction or transfer to other media of any health records. This will be in consultation with health professionals, Head of Information Governance and Legal Services/Data Protection Officer, the Senior Information Risk Owner and the Caldicott Guardian.

4.2 When to Scan

Any physical documentation that falls into the guidelines stated in 4.1 must be scanned and stored onto an NHS system within 72 hours of write up. This includes a quality check of the scanned image, noting of activity carried out and the confidential destruction of the original physical document.

4.3 Preparing documents for scanning

Before the scanning of a document can take place, the following actions must be carried out.

- Assess the condition of the document to ensure that it is not too fragile for scanning, pages are not stuck together or inserts such as post-it notes are not attached to any sheets.
- Any notes attached to the document must be placed on a blank sheet of paper for scanning.
- Remove any staples, paper clips and other document bindings taking care not to damage the original document.
- Ensure anything stuck onto the page is firmly attached and is not obscuring anything underneath.
- Check the physical state of the paper. Ensure all folders are straightened out.
- Ensure all pages are in chronological order.
- For patient or staff files, ensure the front page has the following details:
  - Full Name
  - Date of Birth
  - NHS Number/Employee Reference Number
  - Date of Document.
- Any blank pages must not be removed and must be scanned in the order they appear in the original document.
- Remove any poly pockets/plastic wallets.
- Check that all the information in the document pertains to the same patient (NHS number and DOB). Any misfiled information must be removed and relocated in the appropriate record.

The flow chart in Appendix B can be used as an aide memoire.

4.4 Scanning equipment

All scanning must be carried out using a Trust approved machine. Do not scan any images from a machine that does not belong to Humber Teaching NHS Foundation Trust.

All scanning should be carried out to the following resolution settings: 300 DPI (Dots Per Inch) as a minimum.

4.5 Scanning guidance

Staff scanning records must:

- Scan straight. All documents must be scanned straight and not at an angle. The whole content of the document needs to be viewable, and nothing must be missing on the page of the scanned document.
- Scan all pages of a document - The whole page of the document must be scanned, and nothing must be missing on the page of the scanned document.
- Scan both sides of a page – even if the second side is blank. Blank pages must not be deleted.
- Scan all numbered pages even if blank
- Scan in the original paper size.
- Scan using correct colours of the document.
- Scan to a format that cannot be amended e.g. pdf.
- Upload to the correct electronic patient health record.
- If the scanned health record is too large for the system, the record should be scanned in batches. The document name must indicate that the scan is part X of X.
- For the scanning of health records in SystmOne, upload to the correct file type or contact the IT Service Desk for a new file type to be added to your unit.

4.6 Indexing

All scanned documents and records must include a specific set of metadata. This must include:

- Title of the document – this should be a meaningful title which accurately reflects the document.

The document should then be immediately placed within the appropriate system ensuring the correct electronic record has been identified.

All documents and records must be saved using the appropriate naming convention for the system.

The date the document was scanned and the name of the staff member scanning the document will be captured within audit data.

4.7 Quality control

The quality check of a scanned image must be carried out as soon as the scanning has taken place. To ensure all documents are scanned to a satisfactory quality, staff must ensure:

- Every piece of a document is scanned, including blank pages and double-sided documents.
- Any scanned document is unchanged from its original format. Any amendments or additions made to a document must be made prior to scanning.
- All aspects of the scanned document are legible.
- The scanning guidance in Section 4 is adhered to.

For the scanning of manual health records, the quality check must not be carried out by the member of staff who performed the original scanning. The Quality Assurance Log in Appendix C must be completed. As per 4.1, the scanning of manual health records requires the approval of the IG Group.

Staff must document in the electronic record the date the document was scanned, by whom, who quality checked the document and when the original document was destroyed.

Consider adding a flag to the electronic record advised staff of the availability of a scanned manual health record.

4.8 Security and protection

Records that contain Personal Identifiable Data should only be scanned by staff who are authorised to handle the information.

The scanned images should be immediately quality checked and stored within the correct system. No scanned document should be stored on a shared or personal drive, and/or desktop.

The original document should be confidentially destroyed as soon as possible after storing the scanned document. No persons should keep the paper version for their own needs. If you are unsure about destroying a document, do not scan it. Contact the Trust's Information Governance Team for advice first. There should never be two versions of a document.

Scanning of records should take place in a secure environment where only authorised personnel have access.

Any exceptions to the above must approved by the IG Group.

4.9 Document Retention

All physical documentation should be kept until sufficient quality checks have been carried out on a scanned image.

A scanned document must be securely stored and correctly indexed before destroying a physical record.

A scanned document must be destroyed from the area into which it was originally scanned once it has been appropriately stored.

Original Physical Documents can be destroyed once:

- The scanned image is securely stored on the correct electronic record.
- The scanned Document is correctly indexed and noted
- The scanned Document has been thoroughly quality checked to ensure the electronic version is a true and accurate copy of the original.

Once these checks have been carried out, the original document can now be destroyed. This must be marked alongside the scanned document.

Manual health records must be destroyed in line with the Health and Social Care Record Policy and with the approval of the IG Group. The document management contractor who currently holds the records will ensure that records are destroyed in a confidential manner, accordance with British Security Industry Association (BSIA) & National Association for Information Destruction (NAID) standards. A certificate of destruction will be issued. Any records identified and subsequently destroyed or disposed of (for example transferred to other media) will be marked as such on the patient administration system.

Local health manual health records (records not registered with the Medical Records Team) can be destroyed locally once approved by the IG Group. A copy of the Quality Assurance Log in Appendix C along with any Destruction Certificates must be submitted to the Medical Records Department for retention.

Lloyd George envelopes must not be destroyed and must be kept to meet with the requirements for patient record movement. The creation of Lloyd George envelopes ceased in January 2021.

4.10 Legal admissibility

Any scanned document will be managed in accordance with the Trusts Records Management and Information Lifecycle Policy. The scanned copy will, for legal purposes, become the definitive record and will then be subject to correct records management and retention policies set in place for digital documentation. Scanned documents are admissible in court but can differ depending on the court action. In Criminal cases a certified scanned copy can be used *with* proper authentication including how it was scanned and notations declaring it unaltered. In civil action cases, scanned copies can be produced with the court deciding on the evidential

weight issued to the document. These principles arise from the Civil Evidence Act 1995 and the Policy and Criminal Evidence Act 1984.

5 Monitoring and Compliance

Information Governance will review all scanning incidents and report to the Information Governance Group on a quarterly basis.

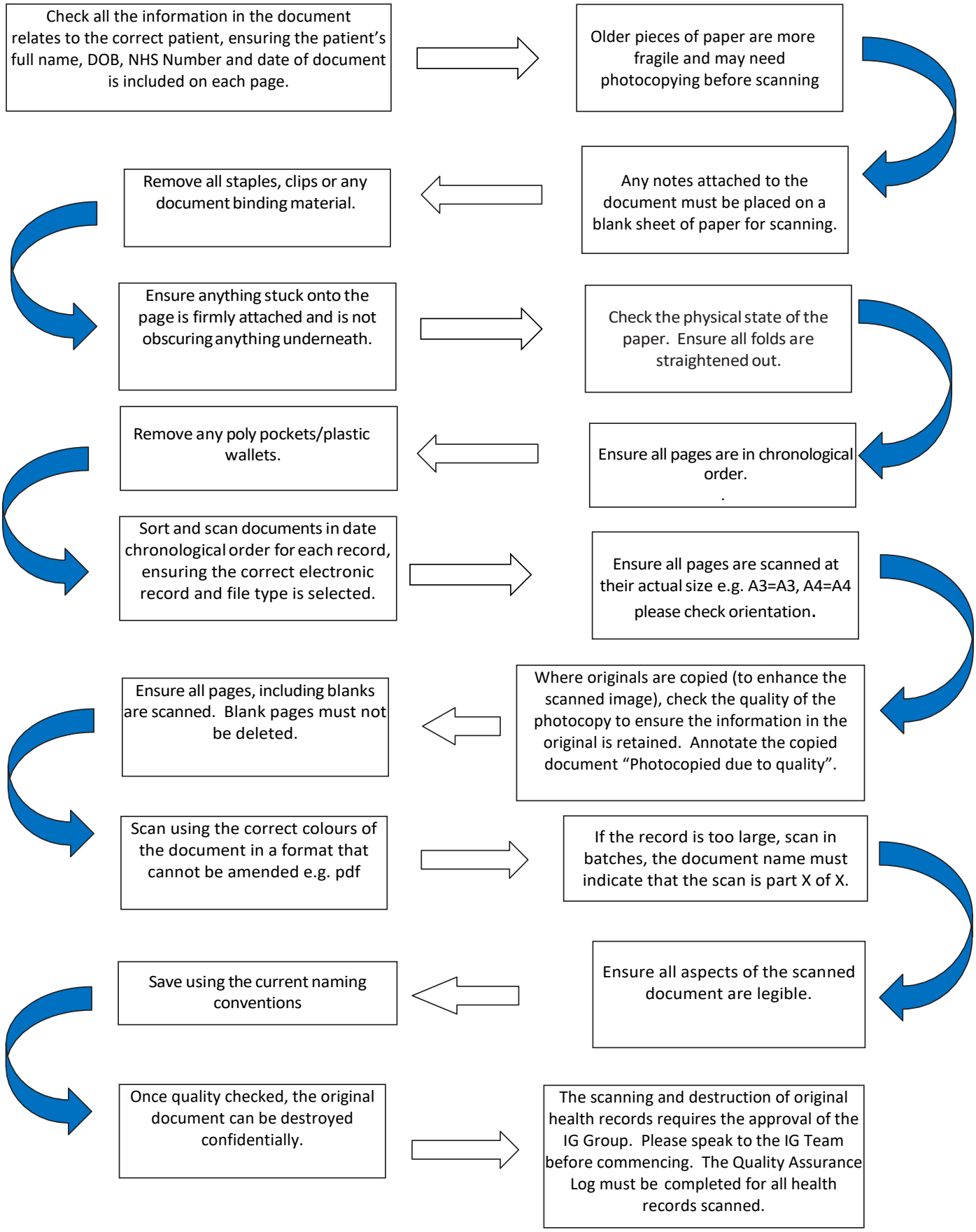
6 Links to associated documents

- Health and Social Care Records Policy
- Records Management and Information Lifecycle Policy

7 References

- Department of Health Informatics Directorate – Information Governance Policy. NHS Information Governance: Records Management – Guidance on Digital Document Scanning (2011)
- NHS X - Records Management Code of Practice 2021
- Digitisation at The National Archives (2015)
- British Standard BS 10008:2008 (2008)
- The Civil Evidence Act (1995)
- Policy and Criminal Evidence Act (1984)

Appendix A: Flowchart



Appendix B Quality Assurance Log Sheet

Humber Teaching NHS Foundation Trust

Scanned Health Records - Quality Assurance Log Sheet

Service:		**EPR:**		**Date range:**	
No of scanned documents in batch:		**Type of health records**	:		

Date scanned dd/mm/yyyy	Name of person scanned/ uploaded document First name, Surname	NHS Number xxx xxx xxxx	Correctly named file on Electronic Patient Record Naming convention	Uploaded to correct patient Y/N	Are all page legible Y/N	Contains all pages Y / N	Issues Y / N	Action(s) Required Detail	Date Corrected dd/mm/yyyy

Checked by (Print name)		**Designation**		**Signed**		**Date**	
Actions completed by (Print name)		**Designation**		**Signed**		**Date**	