



# Clinical Document Scanning Policy and Procedure

This policy describes and defines the processes to be undertaken when scanning documentation onto the Electronic Patient Record (EPR) to ensure adherence to BS 10008 Evidential Weight and Legal Admissibility of Electronic Information.

**Key words:** Scanning, Patient Document, Day Forward, Clinical Documentation, Legal Admissibility, Weight of Evidence, Electronic Records

**Version:** 5

**Approved by:** Data Privacy Group

**Ratified By:** Data Privacy Group

**Date this version was ratified:** July 2024

**Date issued for publication:** 5<sup>th</sup> August 2024

**Review date:** 1 February 2027

**Expiry date:** 31 July 2027

**Type of Policy:** Non-clinical

*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 Trust Website.*

## Contents

SUMMARY & AIM .....	4
KEY REQUIREMENTS .....	4
TARGET AUDIENCE: .....	4
TRAINING.....	4
1.0 Quick look summary.....	5
1.1 Version control and summary of changes.....	5
1.2 Key individuals involved in developing and consulting on the document.....	7
1.3 Governance .....	7
1.4 Equality Statement.....	7
1.5 Due Regard .....	7
1.6 Definitions that apply to this policy. ....	8
2.0 Purpose and Introduction/Why we need this policy.....	9
3.0 Policy Requirements .....	10
4.0 Duties within the Organisation .....	12
5.0 Legal Admissibility.....	15
6.0 Technical requirements .....	16
7.0 Scanning and Quality assurance Processes .....	19
8.0 Monitoring and reporting.....	25
9.0 Retention.....	25
10.0 Risks.....	25
11.0 Disaster Recovery / Business Continuity.....	25
12.0 Mental Health Act Documentation.....	25
13.0 Working files.....	26
14.0 Art/therapeutic materials.....	26
15.0 Copyright materials.....	26
16.0 Training Needs.....	26
17.0 Communication.....	26
18.0 Monitoring Compliance and Effectiveness .....	27
19.0 Standards/Performance Indicators .....	29
20.0 References and Bibliography .....	29
21.0 Fraud, Bribery and Corruption consideration .....	29

*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 Trust Website.*

Appendix 1 Clinical Document Scanning High Level Process .....	29
Appendix 2 Sample Quality Assurance Log -scanned by Clinical Teams .....	30
Appendix 2.1 Sample Quality Assurance Log -scanned by Clinical Document Scanning Team...	31
Appendix 3 Training Needs	
Analysis.....	33
Appendix 4 The NHS	
Constitution.....	34
Appendix 5 Due Regard Screening Template.....	35
Appendix 6 Data Privacy Impact Assessment Screening.....	36

*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 Trust Website.*

# Policy On A Page

## SUMMARY & AIM

The Policy provides assurance to the Trust that where paper-based patient records are reproduced into an electronic version, the legal admissibility and evidential weight will not be affected by the scanning process, by ensuring that staff undertaking the task of scanning check the quality of every scanned image ensuring that authorised scanning capable equipment and defined settings are used. This Policy provides guidance to ensure the authenticity, integrity and legal admissibility of scanned information as per the British Standard 10008:2020 requirements for BIP 0008-1 Code of Practice Legal Admissibility and Evidential Weight of Information Stored Electronically.

## KEY REQUIREMENTS

Staff adequately trained adhering to preparing and scanning processes when scanning within the clinical services for quality assurance checking, using approved scanning equipment and software.

The Clinical Document Scanning Team performing sample quality assurance checks of those documents scanned and the preparation and scanning of clinical documentation for quality assurance checking in line with documented processes.

## TARGET AUDIENCE:

All staff who access, process and / or maintain patient records

## TRAINING

System technical training (SystemOne Scanning) provided by LHIS.

Process training (Clinical Document Scanning) provided on ULearn.

*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 Trust Website.*

## 1.0 Quick look summary

Please note that this is designed to act as a quick reference guide only and is not intended to replace the need to read the full policy.

### 1.1 Version control and summary of changes

Version number	Date	Comments (description change and amendments)
1.0	August 2017	First draft As agreed by Document Scanning Project Board
1.0	October 2017	Final Draft for approval
2.0	April 2019	First revision – removal of procedures and updated with further BIP 0008 information following Stage 1 Audit in March 2019
3.0	March 2020	<p>First revision following successful accreditation to British Standard 10008: 2014:1 Legal Admissibility and Weight of Evidence of Information Stored Electronically, amendments described below:</p> <p>Removal of reference to RiO throughout including any reference to RiO specific functionality such as naming conventions. Key word added to front sheet. Name of responsible committee amended update to contact details. Added &amp; slight rewording within definition table. Section 10. Slight rewording of paragraph 2 &amp; 3.</p> <p>Section 2.0 Slight rewording of bullet point numbers 2, 6 &amp; 8.</p> <p>Section 3.0 Addition to the end of paragraph 4.</p> <p>Section 3.0 Slight amendment to Policy exclusions added.</p> <p>Section 4.2 Paragraph 2 slight rewording to ‘they’.</p> <p>Section 4.4 Changed from Head of Data Privacy.</p> <p>Section 4.6 Addition to end of paragraph.</p> <p>Section 4.7 Addition to end of paragraph.</p> <p>Section 4.8 Addition of paragraph at end outlining line manager responsibility to manage and escalate issues affecting compliance.</p> <p>Section 4.9 slight amendment.</p> <p>Section 5.1 Amended to reflect Trust has achieve compliance and what action must be taken for services not meeting compliance levels required.</p> <p>Section 5.2.1, 6.1 Slight reword of paragraph 2.</p> <p>Section 6.4 Section added to explain in further detail how duplicate correspondence should be managed where the addressee is different and the correspondence refers to multiple subjects.</p> <p>Section 6.5 Addition of Clinical Letters to reflect use of SystemOne functionality.</p> <p>Section 6.6 Slight rewording of paragraph 1 &amp; bullet point 1. Removal of naming convention (RiO only). Slight rewording of bullet point 3 &amp; 4.</p> <p>Section 6.9 New section for system migration.</p> <p>Section 6.11 Revision to scanning timescales</p> <p>Section 6.11 Slight rewording of paragraph 3.</p> <p>Section 7.0 Slight rewording to bullet points 2, 3, 4 &amp; 5</p>

*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 Trust Website.*

Version number	Date	Comments (description change and amendments)
		<p>Section 7.1 Bullet point 1 addition to paragraph 2 to include training, scanner device cleaning measures, slight expansion on the use of long paper setting. Slight rewording &amp; amendment to paragraph 4 to include criminal proceedings and scanner profile tests performed with British Standard test targets (ISO 12653).</p> <p>Bullet point 2 addition to end of paragraph 1.</p> <p>New paragraph added to include safe transportation of documents for scanning; managing items stuck to documents for scanning such as post-it notes; separation and slight expansion for managing documents such as photocopies and document size etc.</p> <p>Section 7.0 – 7.7 Reordering and slight rewording of section.</p> <p>Inclusion of non-conformity process.</p> <p>Addition of incident being recorded for non-return / non action of errors.</p> <p>Addition of expectation for service to check whole batch if 50%+ level of errors found within internal check.</p> <p>Addition of paragraph to explain further sample checking buy Quality Assurance team where 50%+ error level found.</p> <p>Addition of internal audit.</p> <p>Addition of monitoring.</p> <p>Section 8.0 Slight rewording.</p> <p>Section 17.0 added for Communication.</p> <p>Section 18.0 Addition to monitoring to include action for error level over 10%, non- conformity log ,equipment maintenance, SOP competence, internal QA checking, late submissions, escalation of errors not corrected, reportable incidents where documents are missing, on the wrong record or where error documents are not corrected and returned within 4 weeks, ceasing of checking where errors increase <math>\geq 10\%</math>.</p> <p>Section 19.0 Addition of 100% training in EPR &amp; 10008.</p> <p>Removal of appendices 1,3 – all process flow charts are available in the SOP, only the high level process and scan log example is included in the Policy – Appendix 1 &amp;2.</p>
4.0	February 2022	Reviewed with minor amendments to include the overarching Clinical Document Scanning Standard Operating Procedure now in use.
5.0	July 2024	<p>Amendment of BS10008-1:2014 to the updated version of the standard, 2020, therefore known as BS10008-1:2020.</p> <p>Updates following revision of NHSX Records Management Code of Practice for Health and Social Care v7 2021.</p> <p>Addition of the functions of the Scanning Bureau, part of the Clinical Document Scanning Team.</p> <p>Addition of Degradation testing.</p> <p>Update to Training Needs to include system functionality testing.</p> <p>Re insertion of Scanning Timescales.</p>

For Further Information Contact the Records Exploitation Manager.

*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 Trust Website.*

## 1.2 Key individuals involved in developing and consulting on the document

Name	Designation
Claire Mott	Records Exploitation Manager
Sarah Ratcliffe	Head of Data Privacy/Group Data Protection Officer (NHFT/LPT)
Rachel Lowe	Quality Assurance Manager
Hannah Plowright	Data Privacy and Information Governance Manager/Deputy Data Protection Officer
Trust Policy experts	
Members of Data Privacy Group	

## 1.3 Governance

Data Privacy Group.

## 1.4 Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

If you would like a copy of this document in any other format, please contact [lpt.corporateaffairs@nhs.net](mailto:lpt.corporateaffairs@nhs.net)

## 1.5 Due Regard

LPT will ensure that due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and procedures and services are free from discrimination.
- LPT complies with current equality legislation.
- Due regard is given to equality in decision making and subsequent processes.
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 5) of this policy.

*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 Trust Website.*

## 1.6 Definitions that apply to this policy

<b>Batch</b>	A set of paper documents that have been scanned onto the patient electronic record with a usual maximum size of a week's worth of scanned documentation.
<b>Day Forward</b>	Documentation created or received from a specific date onwards.
<b>DPI</b>	Dots Per Inch, a measure of resolution.
<b>Due Regard</b>	Having due regard for advancing equality involves: <ul style="list-style-type: none"> <li>• Removing or minimising disadvantages suffered by people due to their protected characteristics.</li> <li>• Taking steps to meet the needs of people from protected groups where these are different from the needs of other people.</li> </ul> Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.
<b>Electronic Storage</b>	Storage medium or device used by an information management system to store information.
<b>EPR (Electronic Patient Record)</b>	In the Trust this refers to SystemOne. Some patients may have records in multiple SystemOne units concurrently.
<b>Exception</b>	An exclusion from the usual expected process.
<b>Expungement</b>	The process of deleting a document from the system where no evidence of the document ever having been on the system is available.
<b>Legal Admissibility</b>	Evidence to demonstrate that the scanned version is a true representation of the original.
<b>Metadata</b>	Information regarding document structure and properties such as the document type and size. Data regarding data.
<b>Non-Conformity</b>	A failure in the usual conformity of the process.
<b>OCR Optical Character Recognition</b>	Software technology that recognises text within documents in order to search a database for data entry purposes.
<b>Original Document</b>	Document from which a copy is made or from which an image is captured. Original – definition does not mean necessarily original document as we may have a copy of a document it means the original, paper version
<b>Page</b>	Single image entity, such as one side of a sheet of paper, a drawing or plan.
<b>Record</b>	Information created, received and maintained as evidence and information

*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 Trust Website.*



<b>Resolution</b>	Ability of a scanner or image generation device to reproduce the details of an image
<b>Scanner</b>	Device used to capture data of a copied image into a digital file format, e.g. PDF
<b>Scanning</b>	The process that converts the image of a document into a digital form, by detecting the amount of light reflected from elements of a document into a form that is suitable for retrieval, processing and communication by digital computer
<b>SOP</b>	Acronym for Standard Operating Procedure. A standard operating procedure (SOP) is a set of step-by-step instructions compiled by a service to help workers carry out the complex routine of the service SOPs aim to achieve efficiency, and quality output and uniformity of performance, while reducing miscommunication. regulations.
<b>System</b>	In this Policy, this always means the Electronic Patient Record (EPR)
<b>TWAIN</b>	A software driver to enable scanned image direct into other applications i.e. within an EPR such as SystemOne.

## 2.0 Purpose and Introduction

Although the Information Lifecycle and Records Management Policy provides the overarching framework for achieving high quality safe record keeping, it is based on the principle that the primary clinical record is now held in an electronic format which brings many benefits to the care of the patient. The Trust has had a phased implementation of Electronic Patient Records (EPR) with access to trained, authorised staff only. Paper based records are outdated, impractical, unsecure and becoming redundant in the digital era; the rise of EPR and the rise in costs keeping paper for its retention schedule have led to the decision to scan the paper version as an equivalent digital record and destroy. The Trust (LPT) is committed to the use of electronic document storage which has many clinical and financial advantages over paper storage, including ease of access and retrieval and reduction in off-site storage costs. LPT stores documentation received and created outside of the patient EPR onto the patient's relevant electronic patient record. LPT does not use any other stand-alone electronic repository for the storage of patient records to ensure clinical safety.

The Policy provides assurance to the Trust that where paper-based patient records are reproduced into an electronic version, the legal admissibility and evidential weight will not be affected by the scanning process, by ensuring that staff undertaking the task of scanning check the quality of every scanned image ensuring that authorised scanning capable equipment and defined settings are used. This Policy provides guidance to ensure the authenticity, integrity and legal admissibility of scanned information as per the British Standard 10008:2020 requirements for BIP 0008-1 Code of Practice Legal Admissibility and Evidential Weight of Information Stored Electronically.

This Policy is Trust wide and must be adopted with the Standard Operating Procedure (SOP). The SOP will detail all processes required. This Policy defines the system of processes to be adhered to when scanning clinical documentation onto the EPR. The Trust has one EPR in use in scope of this policy and this policy should be reviewed with the Electronic Health Records Policy, Information Security Policies and Information Lifecycle and Records Management Policy.

*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 Trust Website.*

## 3.0 Policy Requirements

The aim of this policy is to ensure that the following objectives are met:

- **Records are available when needed** – all documentation received or created by the service must be scanned and uploaded in line with the Trust's Record Keeping Policy. Similarly any emails or electronic information such as electronic referrals should be uploaded within the same time frame;
- **Records can be accessed** – all information is readily available and readable for those clinicians who need to access it for patient care;
- **Records can be interpreted** – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **Records are secure** – from unauthorised or inadvertent access, alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are protected and held in a robust format which remains readable for as long as records are required;
- **Records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained** – so that all staff are made aware of their responsibilities for record-keeping and record management processes described in this policy and under statute: **The General Data Protection Regulation and Data Protection Act 2018**;
- **Staff understand that it is their responsibility to scan in accordance with this policy** and how to escalate any issues and the implications and ramifications of non-conformity, which may be dealt with under the Disciplinary Policy and Procedure;
- **Staff understand that it is their responsibility to check every document** that is scanned and to use a scanner which is authorised for such purposes.

Within LPT, the task of scanning onto clinical records will be undertaken within each relevant clinical service providing care for the patient or submitted to the Clinical Document Scanning Team for scanning on the EPR. Scanned documentation from Clinical Services submitted to the Clinical Document Scanning Quality Assurance Team for independent Quality Assurance checking as defined within this policy. The objectives will be measured via the production of figures presented in monthly reports as described in section 7.9 Reporting on an ongoing basis. Documentation scanning by the Clinical Document Scanning Team is subjected to Quality Assurance checking by another member of the Clinical Document Scanning Team.

The Clinical Document Scanning Team manage the scanning system processes, however, assistance for technical support with IT equipment/hardware and software (including the EPR)

*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 Trust Website.*

should be sought from the Leicestershire Health Informatics Service (LHIS) through the Service Desk.

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

If this is a record type which must or may be selected and transferred to a place of deposit, the place of deposit should be asked whether they wish to preserve the hard copy and/or the scans. If the hard copy is retained, this will constitute 'best available evidence' for legal purposes, rather than the scanned copy.

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the Courts will interpret evidence can be found in the civil procedure rules and the Court will decide if a record, either paper or electronic, can be admissible as evidence.

The standard, 'British Standard 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information', specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records.<sup>1</sup> This Policy refers to scanned records under British Standard 10008:2020.

<sup>1</sup> IGA Records Management Code of Practice for Health and Social Care 2016

This policy applies to 'day-forward' scanning and ad-hoc scanning of complete medical records held in off-site storage. Scanning of corporate records must follow the same process. The same level of training, internal and external audit are expected to be undertaken by non-clinical services wishing to destroy paper original records. It is expected that a risk assessment would be conducted for each such activity.

The scope of this policy is to ensure that the systems and processes, known as the Electronic Information Management System (EIMS) ensures continued adherence to British Standard 10008:2020. This policy describes the capabilities, system requirements, roles, responsibilities, use of storage technology, the use of compression, the linking of electronic identity, the use of encryption, file formats and the retention and destruction of paper records. The boundaries of the 10008 certification include staff preparing and scanning documentation within the clinical services for quality assurance checking, the Clinical Document Scanning Team performing quality assurance checks of documents scanned, preparing and scanning documentation for quality assurance checking.

The external assurance of scanned documentation (quality assurance check undertaken by the Clinical Document Scanning Team) is dependent on the services provided by the LPT Portering Team and the Leicestershire Health Informatics Service (LHIS) to enable physical and technical functions required to maintain adherence to The Standard. This ensures the best possible solution to the person viewing scanned clinical documentation on the patient record.

Stakeholders and dependencies are displayed in the diagram:

*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 Trust Website.*



Under this policy, all information relating to the care of a service user, received or created outside the EPR, is required to be scanned in order to be added to the EPR across all clinical services in the Trust.

Exclusions from this policy are:

- Complaints from service users
- Patient Advice Liaison Services
- LPT Incident report documentation
- Corporate services
- Police National Computer (PNC) outputs
- Medical Records from other organisations

as this information must not be uploaded to the patient healthcare record.

This Policy applies to the scanning of paper based information onto the clinical record; it does not apply to the electronic transfer of information.

## 4.0 Duties within the Organisation

The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

Trust Board Sub-committees have the responsibility for ratifying policies and protocols.

*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 Trust Website.*

#### **4.1 Chief Executive**

The Chief Executive has overall responsibility for Information Governance and therefore records management within the Trust. As accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. This responsibility is delegated to the Data Privacy Team who oversee record management within the Trust to ensure appropriate, accurate information is available as required.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

#### **4.2 Caldicott Guardian**

The Trust Caldicott Guardian is the Medical Director. They hold the responsibility for safeguarding the confidentiality of patient information and will oversee the arrangements for the use and sharing of patient information due to their responsibility for reflecting patients' interests regarding the use of patient/personal identifiable information

#### **4.3 Senior Information Risk Owner (SIRO)**

The Trust SIRO has responsibility for coordinating the development and maintenance of information risk management policies, procedures and standards for the Trust. They are responsible for fostering a culture for the protection and use of data and act as an advocate for information risk on the Board.

#### **4.4 Data Protection Officer**

The Data Protection Officer has responsibility for ensuring policies are in place for the protection of staff, patient and sensitive organisational information.

#### **4.5 Records Exploitation Manager**

The Records Exploitation Manager has a responsibility to ensure that the all relevant scanning activities within the Trust comply with British Standard 10008:2020 and any other appropriate legislation, through the provision of policy, guidance and instruction to staff who scan clinical documentation and provide advice where required and manage any external audits. The Records Exploitation Manager is responsible for managing and communicating relevant information to users as required. They report to the Governance Manager / Deputy DPO and is responsible for the overall development and maintenance of health records management practices throughout the Trust including the creation and implementation of guidance for good records management practice and promoting compliance with BS10008 in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

#### **4.6 Divisional Directors and Heads of Service**

Divisional Directors and Heads of Service are responsible for ensuring that appropriate standard operating procedures are in place to support and ensure that the scanning of information within their responsible areas are undertaken in line with this policy to ensure the Trust retains compliance with British Standard 10008:2020.

#### **4.7 Senior Managers**

Senior managers are responsible for ensuring that this policy and any supporting policies, standard operating procedures and guidelines are built into local processes and ensure maintenance of compliance to ensure the Trust retains compliance with British Standard 10008:2020.

*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 Trust Website.*

#### 4.8 Line Managers (Information Stewards)

Line Managers are responsible for ensuring that all staff involved in the scanning of clinical documentation are fully aware of this policy and their individual responsibilities. Managers must ensure that staff have undertaken appropriate training to gain access to the EPRs. Managers must ensure that the staff they are responsible for, who are required to scan clinical documents as part of their role, undertake the Clinical Document Scanning Training and pass the assessment before they scan onto a patient record. Managers must ensure the standard operating procedures are followed in line with this policy and the training competency is completed and signed off. Line managers ensure access to the EPR is only granted via Smartcard technology, by an approved Registration Authority Sponsor, once training for the relevant system has been completed. Access is granted via a Smart card which is provided to staff once their identity has been verified. A Smartcard contains technology similar to chip and pin, which is a cryptographic key to ensure secure access. No access is granted prior to training, this ensures that electronic identity can be applied to a document's addition to the EPR. It is line managers' responsibility to ensure that the staff member is competent in both use of the EPR and Clinical Document Scanning including ensuring that scanned documents are successfully uploading onto the EPR (see section 6.1.1) and documents are not left on the system unprocessed. Line managers are responsible for ensuring that their services are achieving the required action and any subsequent measures required such as escalation of issues to senior managers, the retraining of staff etc. Line managers are responsible for local process risk assessments with support from the Clinical Document Scanning Team to ensure the Trust retains compliance with British Standard 10008:2014. Following scanning training (LHIS & Theory on ULearn staff must be signed off and deemed competent locally with local scanning).

#### 4.9 Staff (including Students on placement)

All staff, whether permanent, temporary or contracted, who scan clinical information into patient records should be fully aware of their roles and responsibilities for the secure scanning of clinical information and for ensuring that they comply with these on a day-to-day basis. They are required to complete the Clinical Document Scanning Training via U-Learn and pass the assessment before scanning onto a patient record to ensure the Trust retains compliance with British Standard 10008:2020. Staff must attend the SystmOne Scanning Functionality Training provided by LHIS. ensuring that scanned documents are successfully uploading onto the EPR (see section 6.1.1) and documents are not left on the system unprocessed

Staff must also ensure they remain compliant with mandatory training 'Data Security Awareness' which includes information regarding the Data Protection Act 2018.

#### 4.10 The Clinical Document Scanning Team/Bureau

The Clinical Document Scanning Team/Bureau and the Quality Assurance Manager and team have responsibility of the Scanning function within department to ensure:

- The patient record is available – right patient, right time, right place
- The patient record is scanned to BS10008 standard
- Records are stored, retained and destroyed appropriately

The Scanning Department and staff within clinical services have specific part to play in this through the digitalisation of the paper record by:

- Indexing, preparing, scanning and quality controlling clinical documentation

#### 4.11 Data Privacy Group

*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 Trust Website.*



The purpose of the group is to provide assurance to the Finance and Performance Committee with respect to all aspects of its work program. The group is to lead on the development, delivery and assurance of the Data Security and Protection Agenda for the Trust and to ensure local delivery of its statutory responsibilities. The Group oversees the implementation of the data quality assurance framework and plan, define policy, promote and support the adoption of best practice, monitor compliance, identify emerging patterns in data quality related incidents in order to inform training and influence staff and organisational behaviour. The Group is chaired by the Senior Information Risk Owner (SIRO) or by the Head of Data Privacy/ Data Protection Officer and membership includes the Data Privacy and Governance Manager / Deputy DPO, Records Exploitation Manager and Risk Manager, The Chief Clinical Safety Officer, Clinical Safety Officers as well as representatives from each Clinical Directorate.

## 5.0 Legal admissibility

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

Proving the authenticity of a scanned document is crucial if required as evidence in Court and that any document scanned into or uploaded has not been changed since the time of its storage. For example, a referral letter received by post which is scanned and uploaded to the EPR via a folder on the network is a true representation of the original providing the appropriate processes and quality measures were undertaken when creating the scanned image.

The organisation 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 Legal Admissibility should a Court require it.

Compliance with this procedure does not guarantee legal admissibility. 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, to ensure the best possible evidence can be produced in case of Court proceedings.

### 5.1 Retention of original documentation

Services that do not meet the requirements of British Standard 10008:2020 will be required to ensure their paper copies are retained for respective retention periods; services adhering to British Standard 10008:2020 and meeting Trust objectives will have their paper copies securely destroyed following a short retention period (unless exemption from destruction applies refer to section 7.11).

### 5.2 Legal Implications

The main risk to the Trust, if scanning is undertaken without consideration and implementation of this policy and its requirements, is that the Trust will not be able to prove the integrity of the EPR and that all EPRs may be dismissed as hearsay and therefore not be used as evidence within a Court of Law, Tribunal or Case Review.

The Trust will be required to produce authenticated outputs from the EPR where records are requested and the paper copies have been destroyed.

## 6.0 Technical requirements

*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 Trust Website.*

## 6.1 System size limitations

Documents fewer than 5 MB in size in scanned format can be uploaded as one document to the EPR (SystemOne). There may be a short delay in some EPRs when retrieving documents greater than 1.5 MB in size.

Where one document breaches the system size limitation for upload, it is permissible to scan and upload the record in defined sequential parts ensuring the format Page X of Y is used e.g., Part 1 of 3, Part 2 of 3 etc.

### 6.1.1 Uploading Documents

Staff undertaking scanning must ensure that no documents remain in the 'uploading document' screen as the documents will not be visible to other staff viewing the record. This can be prevented by ensuring that the 'Gateway' is not interrupted on the network for the SystemOne unit whilst scanning and the Gateway PC remains switched on and logged in if documents appear in the uploading document screen. Any computers due for replacement, or where a SystemOne Unit is to be archived, where scanning has occurred, must be checked before replacement or archive as the document will not be retrievable if it has not been fully processed into the patient record. Batches of scanning received for QA checking by the Clinical Document Scanning Team must be submitted with the assurance that none of the documents are pending complete upload to the patient record.

Staff must seek support from the LHMIS Service Desk where required to ensure that all patient documents are fully processed into the patient record and are available for all relevant staff to view.

## 6.2 Use of OCR (Optical Character Recognition) software

OCR technology may be installed and enabled within the EPR for certain functions within the system however, due to accuracy concerns and associated risks, the Trust does not allow the use of OCR technology within patient records including when uploading documents.

## 6.3 Colour Documents

- The following documents must be scanned in colour:  
**ECG's / Prescription cards / DNR sheet / Track & Trigger / NEWS**

This list is not exhaustive; please refer to the local SOP or request a clinical decision if required.

Copies of prescriptions do not need to be in colour.

## 6.4 Duplicate letters

Where duplicate letters e.g., carbon copy letters to different MDT members, are being added to the patient record, either on a single record or shared records, please refer to the services operational process for managing this. Letters addressed to different clinicians (even where the letter content is the same) are not duplicate letters and should be uploaded to the patient record. Documents that have not been scanned should not be submitted for QA check.

Where duplicate letters are for multiple patients i.e., siblings, the relevant number of copies should be taken then the patient NHS numbers and name as minimum 3 items added to each relevant document and uploaded to the correct record. Information should not be obscured or redacted as per record keeping standards.

*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 Trust Website.*



## 6.4.1 Data Entry Forms

Data entry forms where the content is transcribed into the EPR do not require scanning/uploading into the record. The data inputter must satisfy that the data has been transcribed correctly from the paper form and this can be disposed in secure waste.

## 6.5 Letters

### Administrative Letters

Letters of this nature, which do not require a clinical signature (or electronic audit) i.e., an appointment letter, must be created via the EPR and directly saved back into the EPR by the administrative author.

### Clinical Letters

Letters of this nature, which do require a clinical signature (or electronic audit) i.e., an assessment letter, these can be drafted by administrative staff and saved as a draft, the clinician can then review and save as final within the EPR.

## 6.6 Indexing and Metadata

An electronic documents' metadata may contain information about how long the document is, who the author is and when the document was created. Metadata is held in the background of the system and therefore may not be visible to front end users of the system. Some metadata is entered by the user onto the system at the point of adding the document to the patient record, such as:

### ➤ Document type

Pre-defined pick lists of available options are contained within the EPR and the user must select a document type when adding the scanned image to the patient record. Document types are clinically agreed prior to adding to the live EPR.

### ➤ Document date

Appropriate document dates must be entered when the document is uploaded by selecting the appropriate date from the EPR system's calendar. The date may vary according to the content and nature of the document. The following should be observed:

- Document contains clinical intervention date e.g., an Outpatient letter from another hospital: the date of the clinical intervention is to be used
- If there is no clinical intervention date i.e., 'This patient was reviewed recently' then the date of the letter/document is to be used.

If there is neither then the date stamp received or created by the Trust will be used.

If there is no clinical event i.e., an appointment letter, this is to be dated the date of the letter. Future dates cannot be entered into the EPR.

Service exceptions must be raised with the Clinical Document Scanning Team.

### ➤ Document Author

This must be entered as the author of the document. If this is external and is not known, then 'unknown' must be entered. Where there are multiple authors i.e., observation forms completed within an inpatient environment, the name of the ward / home must be used.

## 6.7 Document Storage

*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 Trust Website.*

SystemOne has 2 areas to store items that may not have been created within the EPR: Communications & Letters and Record Attachments. The following guide must be observed:

➤ **Communications & Letters**

This is to be used to store correspondence and documents.

➤ **Record Attachments**

This is to be used to add other file types to the patient record, such as images and medical device output files.

## 6.8 System Migration

Where EPRs are transferred or replaced, or a legacy system is introduced, steps must be taken to ensure that the original metadata is protected and not altered in any way to ensure digital preservation. System upgrade User Acceptance Testing (UAT) must include any implications to the storage of scanned documentation. A risk assessment must be completed to ensure all risks are documented and controlled.

## 6.9 Compression

Compression settings should only be used where there is no loss of information to the scanned version of the document, i.e., lossless compression, which does not remove any aspect of the image. LPT does not use any compression settings other than what is already defined in the scanner profiles to avoid any loss of document / information integrity / outside acceptable limits

## 6.10 Temporary storage of scanned or uploaded documents

Where the document cannot be scanned straight to the EPR (Non-TWAIN complaint) i.e., where the document is too large for a desktop scanner to be scanned using TWAIN driver), a folder must be created within the department/service's network Drive folder; this will be used to temporarily store the scanned documents. If one of the Trust's Multi-Function Devices (MFD) is used, these are defaulted to scan to the email address associated with the staff member's Managed Print Service (MPS) badge or can be set to scan to a secure folder

Once the document has been uploaded the scanned image must be removed from the drive/scanner or email account that the scan was sent to. Staff must not retain any scanned image once it has been successfully uploaded, this will reduce the risk of duplication and ensure start to finish completion of the process. The scanned document must be uploaded to the service user's health care record as soon as is practicably possible after it has been scanned.

These topics are covered in the Clinical Document Scanning Training which is mandatory for staff required to scan onto healthcare records as part of their role.

## 6.11 Scanning Timescales

Scanning of clinical documentation at source sites should occur within 24 hours for Inpatient areas and within 48 working hours for non-inpatient environments. Where areas are not able to meet this, a risk assessment must be undertaken. The Clinical Document Scanning Team will scan batches received within 48 hours to allow for the preparation of large batches received.

Complete documents should be scanned onto patient records unless clinical need necessitates partial documents to be scanned.

Depot / medication cards should be scanned once the card is complete, medication is changed/ discontinued, or the patient is discharged; whichever is sooner.

*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 Trust Website.*

DNAR (Do Not Attempt Resuscitation) forms should be scanned upon patient discharge, with a photocopy of the original form forwarded to the Quality assurance Team, as the original must accompany the patient to their onward destination.

## 7.0 Scanning and Quality assurance Processes

The processes required to comply with British Standard 10008 will include the following stages:

- Preparation to Scan (including training)
- Scanning
- First Level Internal Quality assurance – Quality Control
- Second Level Internal service Quality Assurance Checks
- External Quality Assurance Checks
- Rescanning
- Audit

Flowcharts for each process can be found within the SOP. A high level process flowchart can be found at Appendix 1 in this Policy.

### 7.1 Preparation to Scan

Once staff members are trained in the EPR & associated scanning functionality, have successfully completed, and passed the U Learn training session for Clinical Document Scanning and have completed the SOP Competency, scanning can commence.

#### ➤ Scanning equipment

Only Trust approved scanning equipment must be used. Staff will have access to a desktop scanner or Multi-Function Device (MFD). The use of the LPT scanning profiles is mandated for desktop scanners, other scanning devices e.g., Multi-Function Devices (MFDs) scanning guidance must be followed.

Scanning equipment must be regularly cleaned, maintained, and tested as per service agreements and any issues must be reported to the LHS Service Desk. Desktop scanners should be cleaned monthly by users or as required according to the manufacturer specification and cleaning records should be maintained. Cleaning guidance can be obtained from the Clinical Document Scanning Team. MFDs will be maintained in line with SLA's.

The procurement of scanners must always be completed via the Trust's ordering process.

Only Trust approved scanning profiles must be used, as they enable documents to be scanned and stored in an unchangeable format, users' software does not allow changes to be made to document once it has been scanned. Staff found using software to edit scanned documents will be subject to action under the Trust Performance policy and relevant information security policies and statute where relevant for criminal proceedings. The Trust scanning profiles have been tested with test targets from British Standard ISO 12653 to evaluate the quality of outputs from the

*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 Trust Website.*

scanner. The Clinical Document Scanning Team who perform high volumes of scanning will undertake regular scanner image testing with the test targets.

The relevant SystemOne gateway must be in use within the relevant unit being scanned onto the on the local network that the scanning is being undertaken from.

### ➤ **Document Preparation**

Staff must ensure that each page for scanning is examined and properly prepared as described in the Preparation of Documents Prior to Scanning flowchart in appendix 1 to ensure that as high a quality image as possible is obtained. Staff must follow standards to include the following information as a minimum: DOB, Patient name and NHS number. The Staff member must check the document before adding to the patient record on the EPR; this is the stage that the scanning operative assures that the scanned documents are a true, accurate and complete copy of the original.

Staff must ensure that prior to scanning; documents are transported safely and securely by using appropriate methods i.e., a box file to minimise the risk to the original document's integrity. Any documents presented for scanning with temporary notes (such as a Post It note) must be returned to the clinician for removal. It is not appropriate to scan documents with such items attached. Where this is not possible, the document should be photocopied (using the flatbed) and scanned, then the temporary note removed, and the document scanned without the post it note. The temporary note should be re-attached to the document for submitting to the Clinical Document Scanning Quality Assurance Team.

Documents that are photocopied prior to scanning i.e., the patient has taken the original after it was scanned and we have retained the copy; the photocopy must be marked 'copy' to indicate that the scan is a scanned photocopy of the 'original' version.

Documents must be scanned at their original size e.g. A4, A3 etc. Long paper such as ECG traces can be scanned via the desktop scanners, please seek support from the LHM Service Desk if required to ensure that the 'long paper' setting is enabled on applicable scanners.

## **7.2 Scanning**

Staff must ensure they check every scanned image of the original document once they have scanned it onto the service user's record. Staff must use a Trust approved scanning device set to an authorised profile.

### ➤ **Non-Conformity**

Where the scanning process is interrupted or cannot be completed for example, a document is removed from the batch after it has been scanned as a clinician requests the document before it is sent for QA or a technical issue arises part way through scanning; a non-conformity log (with rationale) must be completed and attached to the relevant documents and submitted separate from the batch to ensure compliance with British Standard 10008:2020.

Non-conformities raised by the Scanning Bureau will be returned to the service where the document cannot be added to the record. An incident report will be opened. Volumes and themes will be reported via the Data Privacy/Quality Group as escalation.

### ➤ **Exception reporting**

*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 Trust Website.*

Where a good quality scan cannot be achieved following 3 attempts using the defined guidance (if for example, the original is of a very poor quality), an exception report must be sent with the document to the Quality Assurance Team separate from the weekly batch. These documents will not be counted as part of any batch. This is to ensure that these are logged and risk assessed for any acceptable limits of information loss or retained. Documents that are not accepted as an exception will be returned to the service for rescanning as appropriate.

Exceptions raised by the Scanning Bureau will be returned to the service where the document cannot be added to the record. An incident report will be opened. Where a risk based decision is made to keep a document raised as an exception, the document will be retained for the relevant retention period.

➤ **Submission of batches**

- Weekly batches of original scanned documentation must sent to the Quality assurance Team within double envelopes/tamper proof envelopes / approved secured and tagged transportation crate, labelled with the service name, relevant SystmOne unit name and scanned date range of documents. A tracking transit form must be used and this will provide a receipt from the collecting porter. Empty boxes (where in use) will be returned to the services once they have been processed.
- Batches of scanned documents sent later than 2 weeks must be submitted with a 100% internal quality check. Batches received after this time affect local error correction rates and can affect the Trust adherence to British Standard 10008:2020.
- Do not mix batches of uploaded documents to different SystmOne units or mix/add to documentation returned with fresh batches.

➤ **Scanning Guidance**

A simple guidance procedure flow chart can be found at Appendix 1. This may be laminated and used as an aide memoire to assist when scanning/uploading documents. Further guides are available on the Intranet and within the SOP

➤ **Role of the Scanning Bureau**

Where the Scanning Bureau undertake scanning on behalf of services, the service must submit regular (weekly unless otherwise agreed) batches of documentation to be scanned. Where a document is deemed a risk to leave the source site it originates from, before being add to the record, this must be scanned at the source site and sent to the Scanning Team for QA checking. Any QA issues discovered by the Scanning Team will be corrected by the Scanning Team. Figures will be reported monthly.

*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 Trust Website.*

## 7.3 First Level Internal Quality Assurance

**Staff must ensure that once a document has been scanned:**

- The document has been uploaded to the correct patient record
- The same number of pages has been scanned and all are the correct orientation to the original (please note, the orientation of blank pages does not matter).
- All pages are legible
- The clinical intervention date is entered as the document date, not the date the document is scanned
- Documents must not be scanned with items such as Post It notes in situ
- The scan is an exact replica of the original paper document
- All documents must be scanned straight and the whole of the document needs to be visible, with nothing missing or covered / obscured on the scanned document.
- Both sides of a page must be included even if the second side of the document is blank – blank pages / sides must not be deleted.
- Documents must be scanned in colour where coloured text, marks or diagrams made on documentation provide a record of clinical care to the patient or holds clinical worth (includes documents on coloured paper).

**This list is not exhaustive - further reasons that a document will fail the quality assurance process can be found within the SOP.**

Once a document is scanned it should not be reprinted for clinical purposes, with the exception of outside agencies / transfer to other Trusts or a Subject Access Request.

## 7.4 Second Level Quality Assurance Checks

Services must carry out an internal quality check on a random sample of batched documents against their scanned images on the EPR

Internal service Quality Assurance Checks are a valuable tool in ensuring the service adheres to processes described in this policy and issues are identified and rectified service level. It also allows team and service level performance monitoring. Managers or peers will perform Quality Assurance checks for 5 – 20% of batches according to service performance. This will be increased where high error rates are prevalent. This should occur before the batch is sent to the central Quality assurance Team for checking in line with British Standard 10008:2020 compliance

The Staff member performing the internal Quality Assurance Checks will select a random sample of the batch and check the paper version against the scanned image. If the image does not match the paper version then the internal Quality Assurance log must be completed as per the process (available in the SOP) and the document must be removed and rescanned where applicable. If errors over 50% are discovered within the local Quality Assurance check, the whole batch must be checked within the service.

Supplementary training is available for staff undertaking Internal Audit Checks on request from the Clinical Document Scanning Team. The documents selected for an internal check must be separated from the rest of the batch and clipped to the log sheet then placed on top of the rest of the batch being submitted.

*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 Trust Website.*



## 7.5 External Quality assurance check

The Clinical Document Scanning Quality Assurance Team will carry out authorised checking processes on the batches of scanned original documents received before either retaining the documents in line with the relevant records retention schedule or until secure destruction can be undertaken.

The Quality Assurance team have 'read only' access to the EPR; this is the required level of access for the role as the team do not make amendments to the patient record. The Quality Assurance team assess the scanned quality by viewing the uploaded document on the EPR against the original or copy (where indicated) paper version.

- The quality assurance check describes the processes, controls and records that the service will put in place to provide assurance that the quality assurance processes are sufficient to successfully catch and therefore remove scanning defects. This does not check documentation for clinical completeness. This will be undertaken by the Clinical Document Scanning Quality Assurance team to assure confidence in the quality control process and to ensure that all pages are legible, the same amount of pages have been scanned and they are exact replicas of the originals. The amount of scanned documentation selected for Quality Assurance checks will be calculated on a risk-based approach and will vary according to performance. The second level checks will be stepped up as required in consultation with service leads. Random increases will also be initiated.
- The Quality Assurance check will also ensure the correct document category is used when saving the document to the patient record to ensure swift clinical retrieval upon review of the patient record.
- The Quality Assurance check will be viewed on the EPR under normal viewing conditions as per the technical specification installed by the Leicestershire Health Informatics Service.
- The Quality Assurance team index all batches received into the team to ensure appropriate tracking of clinical documentation.
- Where a 50% or greater error rate is found within the sample being checked, a further sample will be taken for checking. Where this further check results in another 50% or greater error rate; the service will be informed for their investigation.

All new services submitting documentation to the Clinical Document Scanning Quality Assurance Team will commence at 100% second level checking with reductions following satisfactory audit of check results over an initial 4 week period. The check involves a minimum sample of 20% of the batch up to a maximum of 100%, with a mid-way reduction to 50%. Any services not meeting the requirement maximum error correction rate of **10% and below** will not form part of the Second level Quality Control checking process until this rate can be achieved.

- Second level quality control checks should be undertaken and returned for re-scan or archived within one month. Where this cannot be achieved, services will be informed.
- Training will be provided for staff that perform second level Quality assurance.
- Quality control sheets are completed for every checked batch and must be retained for audit purposes (see appendix 2)
- Documentation that does not meet the Quality standards will be corrected by the Clinical Document Scanning Team.

*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 Trust Website.*

- Documentation that has been uploaded in error / to the wrong record will require removal and adding to the correct record where applicable. An incident will be opened for these occasions.
- The sample size of checks performed will be from a risk-based approach.

## 7.6 Rescanning

Where the scanned image does not meet the requirements the service must correct the error which may include re scanning the document, taking appropriate action to avoid the issue from reoccurring. Staff undertaking scanning must ensure that the results meet Quality Assurance requirements. Only staff with the appropriate access can remove a document from the system; for SystmOne this is 'marked in error' but the document remains accessible within the deleted items node, which staff with an enhanced access role can access. Changes made to documents after upload are held within the audit trail within the EPR. Examples of the types of issues that would result in a rejection during Quality Assurance checks can be found within the SOP.

## 7.7 Audit

### ➤ **Internal – Clinical Document Scanning Team**

The identity of the staff member who was logged onto the system when the document was scanned is held within the EPR within the system audit. The service will need to provide assurance that appropriate procedures are in place to provide evidence that a scanned image is an accurate and unchanged copy of the original and therefore maintains its integrity.

Internal audit of quality assurance checks performed by the Clinical Document Scanning Quality Assurance team occur monthly to ensure that processes as described by this Policy are adhered to within the team. The audits ensure that staff comply with the principles outlined by data protection legislation in addition to compliance with Trust and local policy and SOP. Results of audits will be retained for the duration of the information it pertains to.

The procedure and processes will be audited annually to ensure that procedures are being observed as per the requirements of British Standard 10008:2020. These audits will be undertaken by the Clinical Document Scanning Team and reviewed by the Head of Service.

### ➤ **Internal – Clinical Teams submitting scanning for QA check**

Within Clinical Teams where scanning occurs by staff based within the team, a regular audit of the staff member scanning must be carried out in addition to the completion of the SOP competency to ensure that the processes are adhered to and no new risks present. Guidance and support can be provided from the Clinical Document Scanning Team.

### ➤ **External**

External audit undertaken by the British Standards Institute (BSI) will occur within selected services to ensure the Trust retains certification under British Standard 10008:2020.

### ➤ **Degradation reviews**

*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 Trust Website.*



Periodic checks of accessing and viewing scanned documentation will occur, including after any system down time or changes in scanning software, to ensure documentation is still retrievable. This may result in original paper-based documents being retained for this purpose.

## 8.0 Monitoring and reporting

Team level error correction figures will be provided on a monthly basis to relevant managers and performance charts will be provided at Trust Level. Services are expected to provide assurance for the management of their relevant correction errors. Areas of non-compliance will be investigated to uncover the cause of any issues. Managers are expected to take the appropriate action under the Trusts Performance & Conduct policy where these issues prevail as a direct causation of the scanning errors and staff are accountable for this.

Performance metrics for the Clinical Document Scanning Quality Assurance Team such as volume of scanning, any errors made will be provided to the Data Privacy Group on a minimum of 6 monthly basis. Data for any incidents opened by the Clinical Document Scanning Team will be provided to relevant managers / meetings as required.

## 9.0 Retention

All original documentation will be retained and archived in date boxes once quality control checks have taken place until destruction (exclusions to destruction are documents relating to Huntingdon's or other archival value, research consent forms that must be retained by R&D team or where litigation is suspected or any other documentation that the Trust deems appropriate to retain). All destruction is based on risk assessment.

## 10.0 Risks

Relevant risks and the required controls, mitigation and actions will be held on the Trusts Risk System, Ulysses, for monitoring via the Data Privacy Group. Local services will undertake regular local process risk assessments and share these with the Clinical Document Scanning Team.

## 11.0 Disaster Recovery / Business Continuity

If the EPR is unavailable then the service must follow their local Disaster Recovery Plan. Any documents created during the system being unavailable must be added to the patient record as soon as is practically possible following system reestablishment.

If clinical entries cannot be made within timescales then an incident report must be completed. *This may mean the retention of some patient documentation on site e.g. Emergency Grab sheets, patient demographics as indicated by the services emergency plan. These can be held securely in red temporary file folders.*

## 12.0 Mental Health Act Documentation

The existing processes for Mental Health Act (MHA) related paperwork must be continued. MHA paperwork must not be sent to the central Quality assurance Team but to the Mental Health Act Office (MHAO).

*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 Trust Website.*

### 13.0 Working files

Any assessments that may take more than one clinical contact to complete may be securely fastened and stored in individual labelled red temporary files, until the document is complete and can be scanned in entirety. It is expected that as a minimum, a clinical entry will be made within the EPR which will reference the assessment being undertaken / a summary of the appointment / scan in the partially completed assessment if it is of clinical value to the patient / other clinicians at that point – as per clinical judgement. Once completed the red files can be de-badged and re used for another patient.

### 14.0 Art/therapeutic materials

Images of these can be scanned onto the EPR with patient consent or keep partially completed items in the red file. Upon the patient's discharge, give the document back to the patient unless they request it is destroyed. Enter an entry onto the EPR detailing patient decision to take back or rationale to destroy the item.

### 15.0 Copyright materials

Where copyright explicitly prevents the storage of completed material / documentation, alternate storage arrangements must be sought from the Head of Data Privacy or Data Privacy Manager.

### 16.0 Training Needs

All staff required to scan clinical documentation onto clinical records are required to undertake Clinical Document Scanning Training via the Trusts e-learning platform. This session ensures that staff are fully aware of the principles of this Policy and the processes to be adhered to when undertaking the task of scanning onto clinical records. This training is a one-off session, to be repeated where there are performance issues, a change in post or following return to work after long term absence, as required by management. Records of attendance at training sessions and assessment outcomes will be requested from the workforce team by the team manager. Local managers must ensure that staff members are competent by completing the SOP competency framework and ensuring that local internal quality assurance checks are undertaken.

Training in EPR functionality will be provided by the Leicestershire Health Informatics Service (LHIS) to ensure that staff required to scan onto the EPR as part of their role are fully competent in the use of the functionality. Quick Reference Guides are available as aide-memoirs for the technical aspects of the EPR.

### 17.0 Communication

Regular communications will be distributed by the Clinical Document Scanning Team via the intranet, newsletters, meetings with services/teams, error correction figures are submitted to teams / team managers. There is representation by the Team at forums such as the Data Privacy Group (who the team report into) and IM&TDG in addition to the distribution of incident data and recording of any risks on applicable systems.

*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 Trust Website.*

## 18.0 Monitoring Compliance and Effectiveness

Page/Section	Minimum Requirements to monitor	Method for Monitoring	Responsible Individual /Group	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group). Frequency of monitoring
P11, Section 7	Weekly batches of scanned documentation	Audit	LPT Scanning Team	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P11, Section 7	Minimum check of 20% following reduction from 100% & 50% second level check	Audit	LPT Scanning Team	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P14, Section 7.1	Policy understood, SOP & competency locally completed for each staff member	SOP & Competency sign off	Line Managers	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P14, Section 8	Audit	Audit	LPT Scanning Team / Line Managers	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P15, Section 7	Staff checking paper documentation against the scanned copy	Quality assurance	LPT Scanning Team	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P15, Section 7	Testing of equipment	Testing	Staff member	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P15, Section 7.1	Maintenance of equipment	Cleaning & testing	Staff member	Data Privacy Group, Bi-monthly, Yearly External

*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 Trust Website.*

Page/Section	Minimum Requirements to monitor	Method for Monitoring	Responsible Individual /Group	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group). Frequency of monitoring
				Assessment by British Standards Institute (BSI).
P15, Section 7.2	100% internal check for submitting batches over 2 weeks late	Staff member	Line manager	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P16, Section 7.2	Non-Conformity Log	Reporting of process interruptions	Staff member	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P16, Section 7.4	Internal QA checking	Monitor errors locally	Line Managers	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P17, Section 7.5	Ceasing external QA checks where errors creep up to $\geq 10\%$	Clinical Document Scanning Team	Clinical Document Scanning Team	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P17, Section 7.9	Services to achieve 10% or less error correction rate	Self audit, receipt of Error Correction Figures	Line Managers	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P18, Section 7	Audit	Audit	LPT Scanning Team, Line Managers	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).
P21	Audit data provided for assurance in team performance	Audit	Data Privacy Group	Data Privacy Group, Bi-monthly, Yearly External Assessment by British Standards Institute (BSI).

*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 Trust Website.*

## 19.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
All Trust staff should be aware that the organisation performs comprehensive System access audit trails on a regular basis.	100% of system access audits provide evidence of legitimate and authorised access only.
Adherence and retention of accreditation to British Standard 10008:2020-1 Legal Admissibility and Weight of Evidence of Information Stored Electronically	Internal audit Local error correction figures External audit by British Standards Institute
All staff undertaking Clinical Document Scanning to be trained in both system & 10008 processes	100% of staff to be trained

## 20.0 References and Bibliography

This policy was drafted with reference to the following:

- Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BSI 2020)
- NHSX Records Management Code of Practice for Health and Social Care 2021
- The Civil Evidence Act 1995
- Confidentiality: NHS Code of Practice
- The General Data Protection Regulation and Data Protection Act 2018
- The Electronic Communications Act 2000
- The Computer Misuse Act 1990

## 21.0 Fraud, Bribery and Corruption consideration

The Trust has a zero-tolerance approach to fraud, bribery and corruption in all areas of our work and it is important that this is reflected through all policies and procedures to mitigate these risks.

Fraud relates to a dishonest representation, failure to disclose information or abuse of position in order to make a gain or cause a loss. Bribery involves the giving or receiving of gifts or money in return for improper performance. Corruption relates to dishonest or fraudulent conduct by those in power.

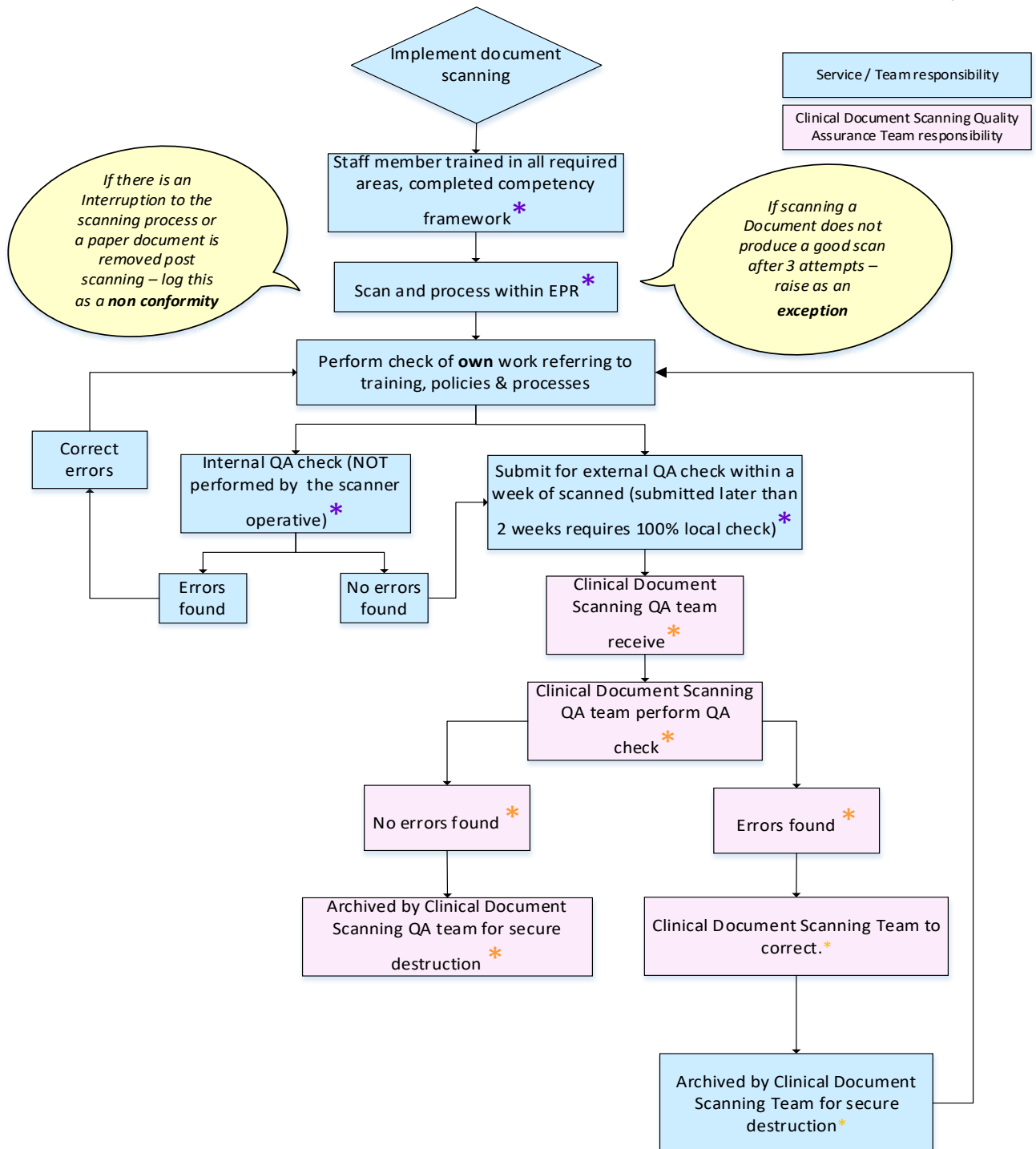
Any procedure incurring costs or fees or involving the procurement or provision of goods or service, may be susceptible to fraud, bribery, or corruption so provision should be made within the policy to safeguard against these.

If there is a potential that the policy being written, amended or updated controls a procedure for which there is a potential of fraud, bribery, or corruption to occur you should contact the Trusts Local Counter Fraud Specialist (LCFS) for assistance.

*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 Trust Website.*

# Appendix 1 Clinical Document Scanning High Level Process

## Colour Key



\*Refer to specific process for services/team

\*Refer to specific process for Clinical Document Scanning Team

CDS\_High Level Process\_v2\_20240320

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 Trust Website.

Clinical Document Scanning Team Quality Assurance Issue Error / Log												
Service:		EPR: SystmOne										
Batch date from:	Batch date to:	Date Received:	Batch number:	Recheck?	If Yes - amount for recheck:							
Total number of scans in batch:	Is a Management check	If yes - management check	Management check %	remainder in batch:	0	Amount checked:	0	Check %	#DIV/0!			
For completion by QA Team								FOR COMPLETION BY SERVICE				
Date	Date Finalised	NHS Number	Document Type (description of document)	Does Document pass QA check? Yes / No	Original document or Copy	Issue Details (allows multiple)	Comment	Staff member who completed the scanning	Errors corrected	Date Corrected		
yyyyymmdd	yyyyymmdd	xxx xxx xxxx		<input type="checkbox"/>	Original / Copy					yyyyymmdd		
Total number of errors			0			Error percentage			#DIV/0!			
Checked by (Sign name):				on behalf of Scanning Quality Assurance Team								
Checked by (print name):												
Date:												

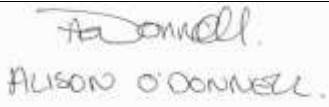
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Quality Assurance Issue Error / Log for Scanning completed by the Clinical Document Scanning Team										
Service:				EPR: <b>SystemOne</b>						
Batch date	Batch date	Date Receive	Batch number:							
Total number of scans in batch:	Scanning Submission	Is a batch scanned and ready for QA checking form enclosed?			Amount checked:		Check % #DIV/0!			
Name of scanner		Number of docs scanned		Date(s) scanned		Name of scanner		Number of docs scanned		
For completion by QA Team										
Date ggggmmdd	Date Finalised ggggmmdd	NHS Number xxx xxx xxxx	Document Type (description of document)	Does Document pass QA check? Yes / No	Original document or Copy Original / Copy	Issue Details (allows multiple)	Comment	SERVICE		
								Staff member who completed the scanning	Errors corrected	Date Corrected ggggmmdd
total number of errors			0		Error percentage			#DIV/0!		
Signed by (Sign name):				on behalf of Scanning Quality Assurance Team						
Signed by (print name):										
Date:										
Print & Sign Name										
Designation:										
Date:										

*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 Trust Website.*



## Appendix 3 Training Needs Analysis

<b>Training topic/title:</b>	<b>1. Data Security Awareness – Mandatory</b> <b>2. Clinical Document Scanning (Desirable or Developmental)</b> <b>3. EPR training (desirable or developmental)</b>		
Type of training: (see Mandatory and Role Essential Training policy for descriptions)	<input type="checkbox"/> Not required <b>1. Mandatory (must be on mandatory training register)</b> <input type="checkbox"/> Role Essential (must be on the role essential training register) <b>2+3. Desirable or Developmental</b>		
Directorate to which the training is applicable:	Yes - Directorate of Mental Health Yes - Community Health Services <input type="checkbox"/> Enabling Services <input type="checkbox"/> Estates and Facilities Yes - Families, Young People, Children, Learning Disability and Autism <input type="checkbox"/> Hosted Services		
Staff groups who require the training: (consider bank /agency/volunteers/medical)	1. All staff 2+3. All staff who scan clinical information into patient records		
Governance group who has approved this training:	<b>Data Privacy Group</b>	Date approved:	July 2024
Named lead or team who is responsible for this training:	Data Privacy Team		
Delivery mode of training: elearning/virtual/classroom/informal/adhoc	1. Elearning 2+3 virtual / face to face		
Has a training plan been agreed?	Yes, in CSTF		
Where will completion of this training be recorded?	Yes - uLearn <input type="checkbox"/> Other (please specify)		
How is this training going to be quality assured and completions monitored?	1. Training Education and Development group monitor compliance 2+3 monitored by Data Privacy Team		
<b>Signed by Learning and Development Approval name and date</b>	 ALISON O'DONNELL.	Date: 12.6.24	

*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 Trust Website.*

## Appendix 4 The NHS Constitution

- The NHS will provide a universal service for all based on clinical need, not ability to pay.
- The NHS will provide a comprehensive range of services.

<b>Shape its services around the needs and preferences of individual patients, their families and their carers</b>	✓
<b>Respond to different needs of different sectors of the population</b>	✓
<b>Work continuously to improve quality services and to minimise errors</b>	✓
<b>Support and value its staff</b>	✓
<b>Work together with others to ensure a seamless service for patients</b>	✓
<b>Help keep people healthy and work to reduce health inequalities</b>	✓
<b>Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance</b>	✓

*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 Trust Website.*

## Appendix 5 Due Regard Screening Template

Section 1			
Name of activity/proposal		Clinical Document Scanning	
Date Screening commenced		05/07/2024	
Directorate / Service carrying out the assessment		Finance and Performance	
Name and role of person undertaking this Due Regard (Equality Analysis)		Claire Mott, Records Exploitation Manager.	
Give an overview of the aims, objectives and purpose of the proposal:			
AIMS: The aim of this policy is to set out how the scanning of clinical documentation will be undertaken within the organisation (Leicestershire Partnership NHS Trust).			
OBJECTIVES: The purpose of this policy is to ensure that standards as defined in British Standard 10008:2020 are adhered to when scanning clinical documentation for the purpose of destroying the original paper based copy.			
Section 2			
Protected Characteristic	If the proposal/s have a positive or negative impact please give brief details		
Age	Positive		
Disability	Positive		
Gender reassignment	Positive		
Marriage & Civil Partnership	Positive		
Pregnancy & Maternity	Positive		
Race	Positive		
Religion and Belief	Positive		
Sex	Positive		
Sexual Orientation	Positive		
Other equality groups?	Positive		
Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click <a href="#">here</a> to proceed to Part B		Low risk: Go to Section 4. ✓	
Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			
This policy defines the processes requiring adherence for the processing of patient clinical documentation and the conversion into scanned images that are legally admissible.			
Signed by reviewer/assessor	CMOTT	Date	05/07/2024
<i>Sign off that this proposal is low risk and does not require a full Equality Analysis</i>			
Head of Service Signed	SRatcliffe	Date	09/07/2024

*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 Trust Website.*

## Appendix 4 Data Privacy Impact Assessment Screening

<p>Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy.</p> <p>The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.</p>		
<b>Name of Document:</b>	Clinical Document Scanning Policy	
<b>Completed by:</b>	Claire Mott	
<b>Job title</b>	Records Exploitation Manager	<b>Date</b> 05/07/2024
<b>Screening Questions</b>	<b>Yes / No</b>	<b>Explanatory Note</b>
<b>1.</b> Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	No	
<b>2.</b> Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
<b>3.</b> Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	No	
<b>4.</b> Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	
<b>5.</b> Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	No	
<b>6.</b> Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	No	
<b>7.</b> As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	No	

*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 Trust Website.*

8. Will the process require you to contact individuals in ways which they may find intrusive?	No	
<p><b>If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via <a href="mailto:Lpt-dataprivacy@leicspart.secure.nhs.uk">Lpt-dataprivacy@leicspart.secure.nhs.uk</a></b>  <b>In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.</b></p>		
<b>Data Privacy approval name:</b>	Sarah Ratcliffe	
<b>Date of approval</b>	09/07/2024	

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust

*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 Trust Website.*