Leicestershire Partnership NHS Trust

# 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 BIP 0008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically as per British Standard 10008:2014.

| | |
|---|---|
| Key Words: | Scanning |
| Version: | 2.0 |
| Adopted by: | Quality assurance Committee |
| Date Adopted: | 21 May 2019 |
| Name of Author: | Scanning Lead |
| Name of responsible Committee: | Data Privacy Steering Group |
| Date issued for publication: | May 2019 |
| Review date: | October 2019 |
| Expiry date: | 1/4/21 |
| Target audience: | All staff who access, process and / or maintain patient records |
| Type of Policy | Non Clinical |
| Which Relevant CQC Fundamental Standards? | 9 & 12 |

# Contents

## 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 |

### For further information contact:

The LPT Clinical Document Scanning Project Team via 0116 295 0898 / 0890.

### 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.

In carrying out its functions, LPT must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which LPT is responsible, including policy development and review.

### Due Regard

LPT must have **due regard** to the aims of eliminating discrimination and promoting equality when policies are being developed. Information about due regard can be found on the Equality page on e-source and/or by contacting the LPT Equalities Team.

## Definitions that apply to this Policy

| | |
|---|---|
| **Day Forward** | Documentation created or received from a specific date onwards. |
| **DPI** | Dots Per Inch, a measure of resolution. |
| **Electronic Storage** | Storage medium or device used by an information management system to store information. |
| **EPR (Electronic Patient Record)** | In the Trust this refers to RiO or SystmOne depending which service(s) the patient is receiving care from. Some patients may have records in multiple systems concurrently. |
| **Expungement** | The process of deleting a document from the system where no evidence of the document ever having been on the system is available |
| **Legal Admissibility** | Evidence to demonstrate that the scanned version is a true representation of the original. |
| **Metadata** | Information regarding document structure and properties such as the document type and size. Data regarding data. |
| **OCR** Optical Character Recognition | Software technology that recognises text within documents in order to search a database for data entry purposes. |
| **Original Document** | 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 |
| **Page** | Single image entity, such as one side of a sheet of paper, a drawing or plan. |
| **Record** | Information created, received and maintained as evidence and information. |
| **Resolution** | Ability of a scanner or image generation device to reproduce the details of an image. |
| **Scanner** | Device used to capture data of a copied image into a digital file format, e.g. PDF |
| **Scanning** | 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 |
| **System** | In this Policy, this always means the Electronic Patient Record (EPR) |
| **TWAIN** | A software driver to enable scanned image direct into other applications i.e. within an EPR such as SystmOne. |

## 1.0. Purpose of the Policy

Although the Record Keeping and Care Planning 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 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 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 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 transferred 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. The policy provides guidance to ensure the authenticity, integrity and legal admissibility of scanned information as per the British Standard 10008:2014 requirements for BIP 0008-1 Code of Practice Legal Admissibility and Evidential Weight of Information Stored Electronically

This Policy is Trustwide and must be adopted into each local Standard Operating Procedure (SOP). This Policy defines the system of processes to be adhered to when scanning clinical documentation onto the EPR. The Trust has 2 EPRs in use in scope of this policy and this policy should be reviewed with the Record Keeping and Care Planning Policy, Information Security Policies and Information Lifecycle and Records Management Policy.

## 2.0. Summary and Key Points

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 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 alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are 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 **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. The scanned documentation will be 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.

The Clinical Document Scanning Team manage the scanning system processes, however, assistance for technical support with IT equipment/hardware and software (including the EPR's) should be sought from the Leicestershire Health Informatics Service (LHIS) through the Service Desk.

## 3.0. Introduction

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 of electronic, can be admissible as evidence.

The standard, 'BS 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.[1]

[1] IGA Records Management Code of Practice for Health and Social Care 2016

This policy applies to 'day-forward' scanning only and does not refer to the scanning of historical records or corporate records. 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) information

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.

### 4.1 Chief Executive
The Chief Executive has overall responsibility for Information Governance within the Trust.

### 4.2 Caldicott Guardian
The Trust Caldicott Guardian is the Medical Director. He has responsibility for safeguarding the confidentiality of patient information and will oversee the arrangements for the use and sharing of patient 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.

### 4.4 Head of Data Privacy
The Head of Information Governance has responsibility for ensuring policies are in place for the protection of staff, patient and sensitive organisational information.

### 4.5 Document Scanning Change Lead
The Document Scanning Change Lead has a responsibility to ensure that the all scanning activities within the Trust comply with BS 10008:2014 and any other appropriate legislation, through the provision of policy, guidance and instruction to staff who scan clinical documentation and provide advice where required.

### 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.

### 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.

### 4.8 Line Managers

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 that standard operating procedures are followed in line with this policy and updated as necessary with the appropriate support of the Document Scanning Change Lead. 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. No access is granted prior to training, this ensures that electronic identity can be applied to a document's addition to the EPR.

### 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 attend the Clinical Document Scanning Training and pass the assessment before scanning onto a patient record.

## 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 fax 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

During the implementation phase of Clinical Document Scanning paper copies will be retained until the Trust has BIP 0008 compliance for their respective retention schedules. Once the Trust achieves compliance, a risk based approach to secure destruction will be deployed.

### 5.2.1 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.

When the Trust commences destruction The Trust will be required to produce authenticated outputs from the EPR where records are requested.

## 6.0 Technical requirements

### 6.1 System size limitations

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

Where a document breaches the system size limitation for upload, it is permissible to scan and upload the record in defined sequential parts, e.g. Part 1 of 3, Part 2 of 3 etc.

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

Due to accuracy concerns and associated risks, the Trust does not allow the use of OCR technology for patient records.

### 6.3 Colour Documents

- The following documents must be scanned in colour:
  **Psychiatric Observations / 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 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.

### 6.5 Administrative Letters

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

### 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 written. Metadata is held in the background of the system and therefore may not be visible. Some metadata is entered onto the system at the point of adding to the patient record, such as:

- **Document type**

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 and categories are clinically agreed prior to adding to the live EPR.

- **Naming convention**

Naming conventions provide a set of rules, which assist the individual end user in allocating a framework for the naming of folders that hold a group of documents. This ensures that documents are accessible, retrievable and readable.

Naming conventions for record titles should aim to:

- Give a unique title to each record
- Give a meaningful title which closely reflects the records contents
- Express elements of the title in a structured and predictable order
- Locate the most specific information at the beginning of the title and the most general at the end
- Give a similarly structured and worded title to records which are linked (e.g. an earlier and a later version)
- Use version control where multiple documents of the same content and date are uploaded.

The Trusts current naming conventions are available on the Intranet and also available within the clinical systems...

➢ **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.

➢ **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, the name of the ward / home must be used.

SystmOne 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:

### 6.7 Communications & Letters

This is to be used to store correspondence and documents.

### 6.8 Record Attachments

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

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.

### 6.9 Compression

Compression should only be used where there is no loss of information, 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. RiO or 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.

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 should occur within 24 hours within Inpatient areas and 2 working days for all other areas. 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.

DNAR (Do Not Attempt Resuscitation) forms should be scanned upon patient discharge, with a copy 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 BS 10008 will include the following stages:

- Preparation to Scan
- Scanning (including re-scanning)
- First Level Quality assurance – Quality Control
- Internal service Management Quality Assurance Checks
- Second Level Quality assurance
- Audit

## 7.1 Preparation to Scan

- **Scanning equipment**

Only Trust approved scanning equipment must be used. Staff will have access to a desktop scanner or Multi-Function Device (MFD).

Scanning equipment must be regularly cleaned, maintained and tested as per service agreements and any issues must be reported to the LHIS Service Desk.

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

Only Trust approved profiles must be used, as they enable documents to be scanned and stored in unchangeable format; software does not allow changes to be made to document. Staff found using software to edit scanned documents prior to storage will be subject to action under the Trust Performance & Conduct policy and relevant information security policies

- **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. The Staff member must check document before adding to EPR: this is the stage that the scanning operative assures that the scanned documents are a true, accurate and complete copy of the original.

## 7.2 Quality assurance Checks

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 scanner set to an authorised profile.

Line managers will carry out an initial quality check on a random sample of batched documents against their scanned images on the EPR before the batch is sent to the central Quality assurance Team for checking in with BIP 0008 compliance

The central Quality assurance Team will carry out authorised checking processes on the batches of scanned original documents received before, either sending the documents to off-site storage for retention in line with the relevant records retention schedule or until secure destruction is approved following BIP 0008 accreditation.

## 7.3 Scanning

- **Staff must ensure that:** Blank pages must not be deleted.
- The use of the LPT scanning profiles is mandated for desktop scanners, other scanning devices e.g. Multi Function Devices (MFD's) guidance must be followed.
- 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).

## 7.4 First Level 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
- They are the exact replicas of the originals
- 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.
- Once a document is scanned it should not be reprinted for clinical purposes, (unless an area which uses paper records requests it) with the exception of outside agencies / transfer to other Trusts or a Subject Access Request.

Training will be provided to all staff undertaking Clinical Document Scanning

### 7.5 Rescanning

- The service must re scan the document, taking appropriate action to avoid the issue. Staff undertaking scanning must ensure that the results meet the requirements of the Quality Assurance. The control sheet and the document must be returned signed to the Quality Assurance team once rescanning is complete and the error has been removed. Only staff with the appropriate access can remove a document from the system; for SystmOne this is marked in error but remains accessible in the deleted items node, which staff with an enhanced access role can only access. For RiO; only application support can removed document which is audited and logged by the LHIS support service database. All clicks in the systems are audited. Documents deleted from RiO are expunged. The scan log must be returned with the correct document for the recheck process.
- The batch must not be added to once it has been processed for the first time by the Scanning Quality Assurance Team. If any documents are removed from the batch i.e. as they should not have been added to the patient record, this must be indicated on the scan log sheet to account for the variation in the batch number once it is returned to the Scanning Quality Assurance Team.

### 7.6 Internal service Management Quality Assurance Checks

Internal service Management 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.

Supplementary training is available for staff undertaking Management Audit Checks.

### 7.7 Second Level Quality assurance check

- Weekly batches of <u>original</u> scanned documentation must sent to the Quality assurance Team within double envelopes / transportation crate, labelled with the service name, and date range of scanned documents. The documentation must be sent in double bagged tamper-proof envelopes / secure transportation tagged crate marked in confidence and receipt obtained from the collecting porter. Empty boxes (where in use) will be returned to the services.
- Do not mix batches of uploaded documents to different SystmOne units or mix/add to documentation returned for re-checking with fresh batches.
- Exception reports (where a good quality scan cannot be achieved following 3 attempts using the defined guidance) must be sent to the Quality Assurance Team separate to the weekly

batch. This is to ensure that these are risk assessed for any acceptable limits of information loss or retained.

**The LPT Quality Assurance Team will undertake the second level check (See Appendix 2).**

- A second level quality control 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 Quality Assurance team to assure confidence in the quality control process and to ensure that the 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 / naming convention is used when saving the document to the patient record to ensure swift 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 Health Informatics Service.
- The Quality Assurance team index all batches received into the team to ensure appropriate tracking of batches.

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 second level check involves a minimum sample of 20% of the batch up to a maximum of 100%, with a mid-way reduction to 50%. All new services commencing the LPT Scanning Project will commence at 100% second level checking with reductions following satisfactory audit of check results over an initial 4 week period.

- Second level quality control checks should be undertaken and returned for re-scan or archived within one month.
- Training will be provided for staff who 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 returned securely to the service via the portering service, which is tracked with a Quality Assurance control sheet which details the error(s).
- Errors that are not rectified after the first return will be raised with the Clinical Document Scanning manager for further review to be raised with the services manager where applicable.
- 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.

### 7.8 Audit

The procedure and processes will be audited annually to ensure that procedures are being observed. The identity of the staff member who scanned the documentation held within the EPR is held within the system audit. The service will need to provide assurance that appropriate

audit trails 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 Second Level checks performed by the Clinical Document Scanning Quality occur monthly to ensure that processes as described by this Policy are adhered to within the Document Scanning Quality Assurance Team.

### 7.9 Reporting

Team level figures will be provided on a monthly basis to relevant managers and performance charts will be provided at Trust Level. 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.

### 7.10 Scanning Guidance

A simple guidance procedure for scanning and uploading documents can be found at Appendix 1. This may be laminated and used as an aide memoire to assist when scanning/uploading documents. Scanning good practice reminders are issued following successful completion of training.

### 7.11 Retention

All original documentation will be retained and archived at C&V in date boxes once quality control checks have taken place for the document respective retention schedule. Once the Trust has achieved BIP 0008-1 compliance and a fully informed risk based assessment has been undertaken, destruction will the original documents will be securely destroyed (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).

## 8.0 Risks

A Risk Log describing all relevant risks and the required action will be held on the Clinical Document Scanning Intranet page. Risks will be recorded on the Trusts' risk management software, Ulysses, as appropriate.

## 9.0 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.*

## 10.0 Mental Health Act Documentation

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

## 11.0 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 entirely. 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.

## 12.0 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 destroy the item.

## 13.0 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.

## 14.0 Training Needs

All staff required to scan clinical documentation onto clinical records are required to undertake Clinical Document Scanning Training. 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 retained by the Clinical Document Scanning Team manager.

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.

## 15.0 Monitoring Compliance and Effectiveness

| Ref | Minimum Requirements | Evidence for Self-assessment | Process for Monitoring | Responsible Individual / Group | Frequency of monitoring |
|---|---|---|---|---|---|
| P14 | Staff checking paper documentation against the scanned copy | Section 8.3.1 | Level 2 Quality assurance | LPT Scanning Team | Monthly |
| P11 | Weekly batches of scanned documentation | Section 8.4 | Audit | LPT Scanning Team | Monthly |
| P11 | Minimum check of 20% following reduction from 100% & 50% second level check | Section 8.4 | Audit | LPT Scanning Team | Monthly |
| P18 | Audit | Section 8.8 | Audit | LPT Scanning Team | Monthly |
| P15 | Testing of equipment | Section 8.1 | Testing | Staff member | 6 monthly |
| P14 | Audit | Section 8 | Audit | LPT Scanning Team / Line Managers | 3 monthly |

## 16.0 Standards/Performance Indicators

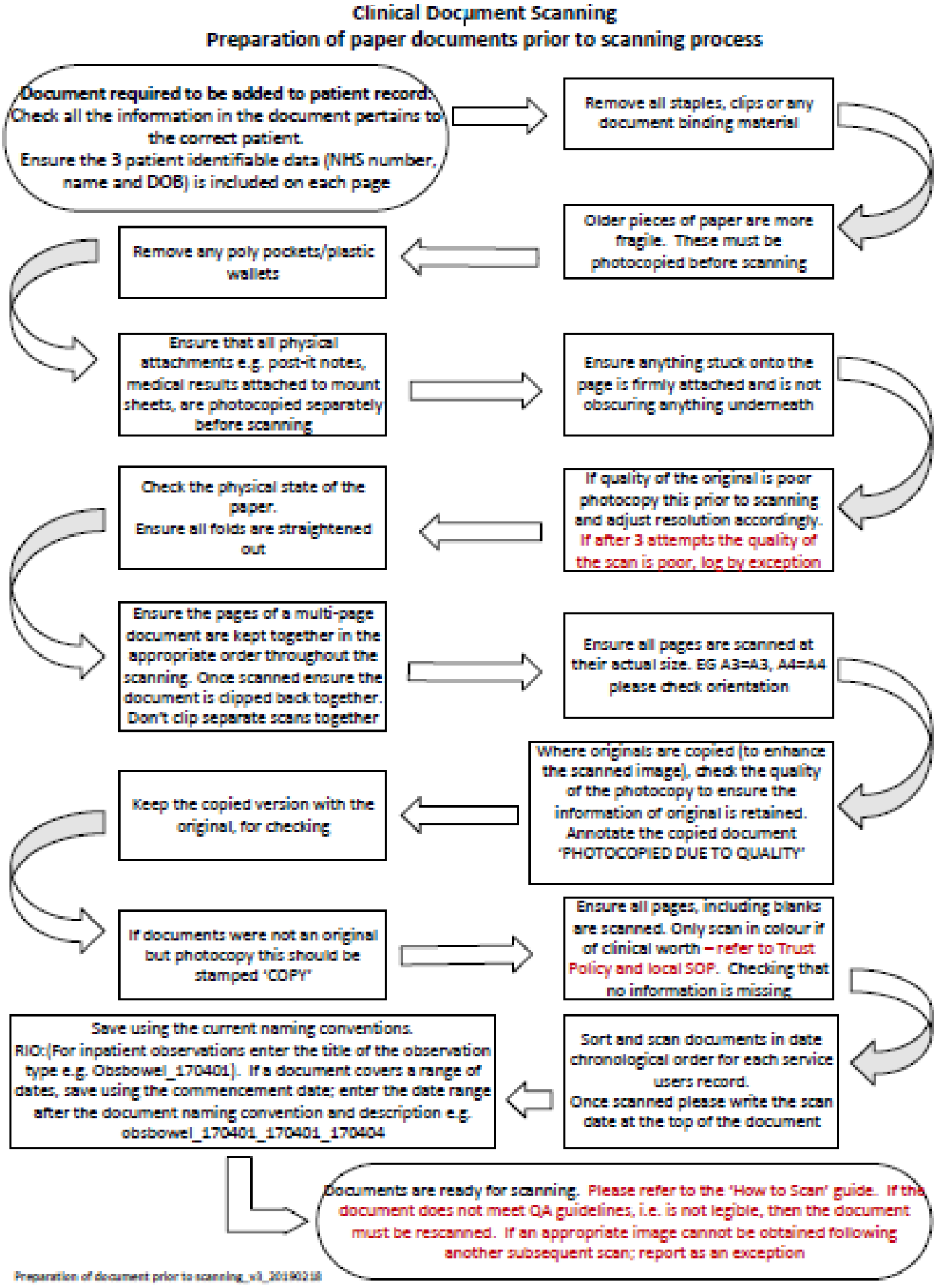
| TARGET/STANDARDS | KEY PERFORMANCE INDICATOR |
|---|---|
| All Trust staff should be aware that the organisation performs comprehensive system access audit trails on a regular basis | 100% of system access audits provide evidence of legitimate and authorised access only |

## 17.0 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 2014)
- IGA Records Management Code of Practice for Health and Social Care 2016
- The Civil Evidence Act 1995
- Confidentiality: NHS Code of Practice
- The General Data Protection Regulation 2018
- The Electronic Communications Act 2000
- The Computer Misuse Act 1990

**Appendix 1**


Clinical Document Scanning
Preparation of paper documents prior to scanning process
Document required to be added to patient record: Check all the information in the document pertains to the correct patient. Ensure the 3 patient identifiable data (NHS number, name and DOB) is included on each page
Remove all staples, clips or any document binding material
Older pieces of paper are more fragile. These must be photocopied before scanning
Remove any poly pockets/plastic wallets
Ensure that all physical attachments e.g. post-it notes, medical results attached to mount sheets, are photocopied separately before scanning
Ensure anything stuck onto the page is firmly attached and is not obscuring anything underneath
Check the physical state of the paper. Ensure all folds are straightened out
If quality of the original is poor photocopy this prior to scanning and adjust resolution accordingly. If after 3 attempts the quality of the scan is poor, log by exception
Ensure the pages of a multi-page document are kept together in the appropriate order throughout the scanning. Once scanned ensure the document is clipped back together. Don't clip separate scans together
Ensure all pages are scanned at their actual size. EG A3=A3, A4=A4 please check orientation
Keep the copied version with the original, for checking
Where originals are copied (to enhance the scanned image), check the quality of the photocopy to ensure the information of original is retained. Annotate the copied document 'PHOTOCOPIED DUE TO QUALITY'
If documents were not an original but photocopy this should be stamped 'COPY'
Ensure all pages, including blanks are scanned. Only scan in colour if of clinical worth – refer to Trust Policy and local SOP. Checking that no information is missing
Save using the current naming conventions. RIO:[For inpatient observations enter the title of the observation type e.g. Obsbowel_170401]. If a document covers a range of dates, save using the commencement date; enter the date range after the document naming convention and description e.g. obsbowel_170401_170401_170404
Sort and scan documents in date chronological order for each service users record. Once scanned please write the scan date at the top of the document
Documents are ready for scanning. Please refer to the 'How to Scan' guide. If the document does not meet QA guidelines, i.e. is not legible, then the document must be rescanned. If an appropriate image cannot be obtained following another subsequent scan; report as an exception
Preparation of document prior to scanning_v3_20190218

**Appendix 2** **Sample Quality assurance Log Sheet**

| Quality assurance Team QUALITY ASSURANCE Check Log | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Service:** | | | | **EPR:** | | | | | | | |
| **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 enclosed?** | | **If yes - management check amount:** | | **Management check %** | | **remainder in batch:** | | **Amount checked:** | | **Check %** | |

| For completion by QUALITY ASSURANCE Team | | | | | | | | | | FOR COMPLETION BY SERVICE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Document date**<br>**yyyymmdd** | **Document received date / date on EPR (if applicable)**<br>**yyyymmdd** | **NHS Number**<br>**xxx xxx xxxx** | **Correctly named file on Electronic Patient Record**<br>**Y/N** | **Document Type (description of document)** | **Uploaded to correct patient**<br>**Y / N** | **Original document or Copy**<br>**Original / Copy** | **Issues**<br>**Y / N** | **Issue Details (allows multiple)** | **Comment** | **Document removed from batch? Y/ N (service to complete)** | **Reason for removal from batch** | **Date Corrected**<br>**yyyymmdd** |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| | |
|---|---|
| **Checked by (Sign name):** | |
| **Checked by (print name):** | |
| **Date:** | |

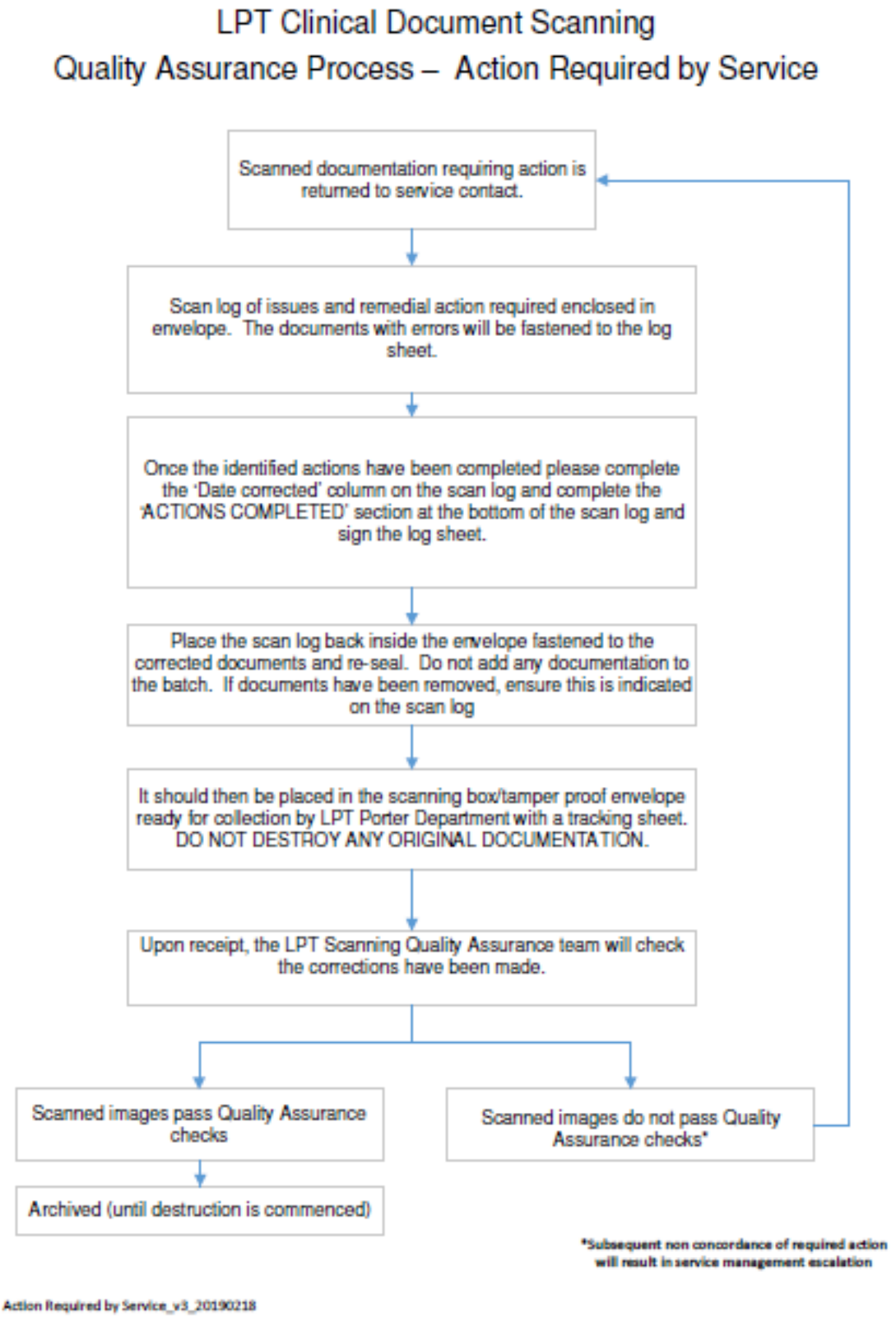
**on behalf of Scanning Quality assurance Team**

## ACTIONS COMPLETED (to be completed by Service):

| | |
|---|---|
| **Print & Sign Name** | |
| **Designation:** | |
| **Date:** | |

**Appendix 3**

## Quality assurance Second Level Check Process



**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**

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

**Appendix 5**

## Stakeholders and Consultation

### Key individuals involved in developing the document

| Name | Designation |
|---|---|
| Sam Kirkland | Head of Data Privacy |
| Mary Stait | Data Privacy Manager |
| Claire Mott | Clinical Systems Change Manager |
| Rachel Lowe | Information Request Officer |

### Circulated to the following individuals for comment

| Name |
|---|
| Members of Data Privacy Steering Group |

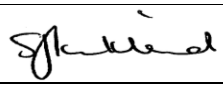
**Appendix 6**

## Due Regard Screening Template

| **Section 1** | |
|---|---|
| **Name of activity/proposal** | Clinical Document Scanning Policy |
| **Date Screening commenced** | 30 October 2017 |
| **Directorate / Service carrying out the assessment** | Quality and Professional Practice |
| **Name and role of person undertaking this Due Regard (Equality Analysis)** | Claire Mott, Clinical System Change Manager |
| **Give an overview of the aims, objectives and purpose of the proposal:** | |
| **AIMS:**<br>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:**<br>The purpose of this policy is to ensure that standards as defined in BIP 0008 BS 10008:2014 are adhered to when scanning clinical documentation for the purpose of destroying the original 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 here 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** | | **Date** | 30 October 2017 |
| *Sign off that this proposal is low risk and does not require a full Equality Analysis* | | | |
| **Head of Service Signed** |  | **Date** | 1 November 2017 |

## Appendix 7

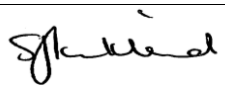
### DATA PRIVACY IMPACT ASSESSMENT SCREENING

**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.**
**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.**

| | | |
|---|---|---|
| **Name of Document:** | **Clinical Document Scanning Policy** | |
| **Completed by:** | **Claire Mott** | |
| **Job title** | **Change Lead** | **Date 05.04.2019** |

| **Screening Questions** | **Yes / No** | **Explanatory Note** |
|---|---|---|
| **1.** 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 | |
| **2.** 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 | |
| **3.** 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 | |
| **4.** 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 | |
| **5.** 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 | |
| **6.** 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 | |
| **7.** 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 | |
| **8.** Will the process require you to contact individuals in ways which they may find intrusive? | No | |

**If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk**
**In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.**

| | |
|---|---|
| **Data Privacy approval name:** | Sam Kirkland -  |
| **Date of approval** | 05/04/2019 |

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