Leicestershire Partnership NHS Trust

Data Quality Policy

The aim of this document is to identify the intentions of Leicestershire Partnership NHS Trust (LPT) in assuring the quality of information which supports its business.

Key Words:	*Data quality, information*	
Version:	V.5	
Adopted by:	Trust Policy Committee	
Date this version was Adopted:	08/11/2023	
Name of Author: *(Job Title)*	Prakash Patel, Head of Information	
Name of responsible Committee:	Data Quality Committee	
Please state if there is a reason for not publishing on website	N/A	
Date issued for publication:	*November 2023*	
Review date:	*May 2026*	
Expiry date:	*November 2026*	
Target audience:	*e.g. nurses, doctors or all managers*	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?	Good Governance	

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
V1.0	05/12/2017	New policy to reflect national guidance – information governance toolkit/ quality account/ NHS Improvement single oversight framework etc.
V2.0	01/02/2019	Section 5 – Duties within the organisation updated to include 'validation' techniques as recommended by 360 Assurance
V3.0	03/01/2020	Inclusion of data quality flag assessment Inclusion of Business Team responsibilities Update of policy names
V3.1	13/04/2020	Inclusion audit recommendations: - Information Team to respond to training requirements when requested (5.9)
V3.2	26/07/2020	Updated Head of Information contact details
V3.3	31/01/2023	Reviewed and updated
V4	02/06/2023	Review and amendment of policy

For further information contact:
Data Privacy Team *lpt.dataprivacy@nhs.net*

1.0 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.

1.1 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 4) of this policy

2.0 Definitions that apply to this Policy

AMH.LD	Adult Mental Health and Learning Disabilities
CDS	Commissioning Data Sets
CHS	Community Health Services
CQC	Care Quality Commission
DHSC	Department of Health & Social Care
DQ	Data Quality
DQIP	Data Quality Improvement Plan
Due Regard	Having due regard for advancing equality involves: - Removing or minimising disadvantages suffered by people due to their protected characteristics. - Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. - Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.
ETL	Extract Transform Load
FPC	Finance and Performance Committee
FYPC	Families Children and Young People's Services
HES	Hospital Episode Statistics
HIS	Health Informatics Service
HPA	Health Protection Agency
IAA	Information Asset Administrator
IAO	Information Asset Owner
IM&T	Information Management and Technology
BPR	Board Performance Report
ISN	Information Standards Notification
IT	Information Technology
KPI	Key Performance Indicators
LLR	Leicester, Leicestershire and Rutland
LPT	Leicestershire Partnership NHS Trust
MDS	Minimum Data Set
POM	Patient Outcome Measure
QAC	Quality Assurance Committee
SDCS	Strategic Data Collection Services
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SOP	Standard Operating Procedure/ Process
SUS	Secondary User Service

3.0 Purpose of the Policy

The aim of this document is to identify the intentions and outline the expectations of Leicestershire Partnership NHS Trust (LPT) staff in assuring the quality of information which supports its business. Specifically, that is:

- Information that enables effective and timely communication regarding service users and their family/ carers, finances and staffing;
- Information upon which the Trust Board, directorates and stakeholders rely on to monitor and/ or manage LPT's performance in all aspects of its business, including but not explicit to patient activity data, finance and staffing;
- Information that supports and complies with the National Data Guardian 10 Standards, information quality assurance, NHS Data Dictionary and information standard notices (ISN).

4.0. Summary and scope of the Policy

All Leicestershire Partnership NHS Trust internal and published performance information will be subject to the same level of scrutiny.

- Those who collect and/ or record data are responsible for ensuring that it is of a known degree of accuracy through procedures, validation, training and monitoring.
- The responsibility is on individual teams and services to consider the adequacy of their own standard operating procedures (SOPs) for data collection and record keeping. If a significant risk is identified details should be recorded on the risk management system.
- Those who interpret and collate data are responsible for putting in place the necessary procedures, checks and approvals to ensure the reported information is correct.
- Those with executive responsibility for data are responsible for ensuring appropriate process are in place locally to assure them of data accuracy prior to authorising the release of any information externally.

5.0 Introduction

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

5.2 The **Finance and Performance Commitee** is mandated on behalf of the Trust Board to adopt policies

5.3 **Trust Board Sub-committees** have the responsibility for agreeing policies and protocols.

5.4 **Data Quality Committee** is responsible for

- Review, approve and ensure compliance to monitoring and effectiveness standards for all policies that fall under the remit of the committee.
- Agree and oversee the Trust's Data Quality work programmes including the monitoring of the annual Data Quality Plan for the Trust.

- Provide a focal point for the resolution and/or discussion of Data Privacy and Data Quality issues through regular reporting and monitoring.
- Receive summaries and action points from any Task & Finish and Sub-Groups that have been identified to support the work of the group, provide support to these Groups where necessary and seek assurance of compliance from them. To also review the work of the Groups, on a rolling programme.
- Communicate exceptions and risks to Finance and Performance Committee and Strategic Executive Board, where appropriate
- Maintain and make available for Finance and Performance Committee, a work plan of planned assurance activities.

5.5 **Directors of Services/ Information Asset Owners (IAO)** have the responsibility to:

- be accountable for the data which is recorded within their directorate. This will be achieved through formally establishing the 'Performance and Accountability Framework';
- ensure appropriate systems and processes are in place to provide assurance of **reliability**, **timeliness**, **completeness**, **accuracy** and **relevance** of data/ information;
- ensure all of their staff are fully aware of their obligations in these areas;
- provide authority to release information externally (this may be delegated to a named service head);
- manage performance for their area of accountability;
- manage associated risk(s) as appropriate.
- Be accountable for supporting the Trust to meet its Information Standards Notice Compliance through providing resources and skills as required.

5.6 **Heads of Service** have the responsibility to:

- ensure staff members are fully aware of and comply to the standard operational procedures (SOPs);
- ensure that competency in use of electronic systems features as an element of performance appraisal for relevant staff;
- ensure quality assurance processes (SOPs, PTLs, performance reviews etc.) are in place to assure the directorate of the quality of data and information used for external reports from a service perspective;
- ensure processes are in place to measure data quality using the data quality flag criteria on a minimum six-monthly basis. This can be via appraisals, clinical supervision, job planning etc.;
- manage/ escalate significant data quality risk as appropriate.

5.7 **Managers and Team Leaders** have the responsibility to:

- implement and regularly review standard operational procedures (SOPs);
- agree relevant system configuration, local reporting and KPIs for their service(s);
- review data quality reports and remove barriers to resolve issues in a timely fashion;
- implement data quality assurance processes (SOPs, PTLs, performance reviews etc.);
- implement data quality reviews with staff (appraisals, clinical supervision, job planning etc.);
- identify significant or emerging data quality risks and manage/ escalate these as appropriate.

5.8 **All Staff** have the responsibility to:

- follow locally agreed standard operating processes (SOP);
- record patient information into clinical systems in a timely manner as per the Electronic Health Records Policy;
- review data quality reports and resolve issues in a timely fashion;
- identify their own training needs;
- identify significant or emerging data quality risks and escalate these as appropriate.

5.9 **Service Managers** have the responsibility to:

- support the development of standard operating processes (SOPs);
- support the design of KPIs and system configuration to meet the needs of the business;
- manage the implementation and performance management of directorate data quality improvement programmes.

5.10 **Integrated Information Team** (Corporate Service) have the responsibility to:

- review and update the data quality policy;
- provide expert advice to services on good data management practices;
- provide information training/ support as identified by staff;
- ensure that supporting reports relating to data quality are produced accurately and are accessible;
- agree and implement robust data/ report authorisation and release procedures;
- ensure externally shared data/ reports meets the requirements of trust information governance procedures;
- ensure the timely creation and submission of reports;
- highlight areas of poor data quality to the service for resolution;
- identify significant or emerging data quality risks and manage/ escalate these as appropriate;
- provide expert stakeholder advice and safeguard the integrity of trust data in the event of system change;
- ensure all changes required by external agencies for data provided by the trust are actioned in a timely and consistent manner (e.g. ISNs);
- ensure that information on changes in guidelines and data definitions is provided to the services and HIS for local procedures to be amended;
- manage audit programmes to establish the integrity of the clinical system data and report the results of those audits to relevant groups.

5.11 **Clinical Coding Assurance Team** (Corporate Service) have the responsibility to:

- Provide accurate, complete, timely coded clinical information to support Commissioning, national and local information requirements i.e. Mental Health Services Data Set (MHSDS) and central returns on behalf of the Trust.
- The International Classification of Diseases 10th Revision, commonly known as ICD-10, has been devised by the World Health Organisation (WHO) and its codes, which cover all reasons for patients' admissions to hospital, and are widely used internationally.
- The codes included in the Office of Population Censuses and Surveys 4th Revision,

commonly known as OPCS4, cover all operative procedures and interventions that patients have undergone during their hospital stay. These codes are used in the United Kingdom only.

- To input onto the trust information system accurate and complete clinical coding information within 10 days of discharge/transfer to support the information requirements of the Trust and Commissioners.
- To provide accurate, consistent, and timely information to support clinical governance and data quality.
- Focused data quality audit on clinical coding is a crucial part of a robust assurance framework and guidance from Standard 1 of the DSPT stipulates that it must be audited either via a continuous programme or via a single audit annually.
- Provide single point reference for SNOMED implementation. And offer assurance for successful outcome of project.

5.12 **LHIS Systems Change Team** (Hosted Service) has the responsibility to:

- ensure systems are configured to accurately record clinical activity, to minimise manual actions and to minimise data quality issues.
- ensure that the Trust is able to meet the requirements laid out with the annual Data Quality Action Plan
- ensure systems are configured to meet national standards; and that requirements for national standards are monitored and included in annual work plans.
- ensure all requested changes follow the single clinical system change process and ensure changes are authorised by all relevant stakeholders prior to implementation;
- support the development of SOPs across the trust;
- Respond to requests from services to assist in the maintenance of data quality In accordance with the Trust data quality priorities and local and national reporting requirements

5.13 **LHIS Data Warehouse Team** (Hosted Service) has the responsibility to:

- ensure all business rules are applied to data held in the warehouse.
- ensure the Trust's data and any other local/ national reference tables as required are migrated from clinical systems to our data warehouse where it is stored and processed optimally
- ensure data items are available on a daily basis.
- clearly communicate and resolve data failures, data loss and/ or data anomalies as part of the extract, transform and load (ETL) process in a timely manner.
- create clinical system reports to support data quality and operational management;
- create, maintain and support ad-hoc data collection tools/ systems in line with the HIS SLA.

5.14 **LHIS Application Training Team** (Hosted Service) has the responsibility to:

- provide clinical system training; that supports the Trust to deliver the annual Data Quality Plan and ensuring that users are provided the appropriate tools to capture high quality information at the point of care
- to manage the system change process in accordance with Trust policy and process

5.15 **Clinical Staff** have the responsibility to:

- Clinical staff must ensure that consent has been sought and obtained before any care, intervention or treatment described in this policy is delivered. Consent can

be given orally and/ or in writing. Someone could also give non-verbal consent as long as they understand the treatment or care about to take place. Consent must be voluntary and informed and the person consenting must have the capacity to make the decision.

- In the event that the patient's capacity to consent is in doubt, clinical staff must ensure that a mental capacity assessment is completed and recorded. Someone with an impairment of or a disturbance in the functioning of the mind or brain is thought to lack the mental capacity to give informed consent if they cannot do one of the following;
- Understand information about the decision
- Remember that information
- Use the information to make the decision
- Communicate the decision
- Ensure information is adequate, relevant and up to date

6 The Health Record and Clinical Coding

A health record is defined in the Data Protection Act 2018 as a record which consists of data concerning health, and has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates. The health record can be held partially or wholly electronic or on paper. The health record (commonly referred to as the medical record and used hereafter) is the source documentation for the purposes of clinical coding.

The responsible consultant, or healthcare practitioner, is accountable for the clinical information they provide. It must accurately reflect the patient's encounter with the health care provider at a given time. The clinical coder expects to find all relevant clinical information in the medical record and attributed to the relevant consultant episode within the hospital provider spell. The structure and contents of the medical record may vary from hospital to hospital.

Typically, there are handwritten notes, computerised records, correspondence between health professionals, discharge letters, clinical work-sheets and discharge forms, nursing care pathways, histology reports and diagnostic test reports. Any of these sources may be accessed for coding purposes. The accuracy, completeness and legibility of the medical record are critical to the assignment of the correct ICD-10 code(s) and the production of consistent, high quality information and comparable data to manage health and care.

In the case of post-mortem reports these should always be processed through the responsible consultant in preparation of a summary. Use of the post-mortem report should, therefore, be the responsibility of the responsible consultant, who should decide what goes into the clinical summary for the coder. When the medical record does not contain sufficient information to assign a code, the clinical coder must consult the responsible consultant (or their designated representative3).

The national clinical coding standards cannot provide direction to compensate for deficiencies in the documentation, recording or coding process. The clinical coding manager should use the local information governance and clinical governance arrangements to address documentation and recording issues to support data quality improvements that will generate aggregate data that are valid and comparable.

7.0 Overview of Process/ Procedure

Information is processed through seven key stages, each of which has procedures, checks and measures to ensure a high-level data quality (see flow- diagram in Section 12):

- Standard Operating Processes (SOPs)
- System Change (optimisation)
- Data Input (Record Keeping)
- Data Validation
- Data Warehouse
- Information Delivery
- Performance Review, Authorisation and Submission
- Bi-monthly data quality highlight reports to Data Quality Committee

7.1 Standard Operating Processes (SOPs)

Standard operating processes (SOPs) are the service specific processes which clearly determine how and when information is entered onto clinical systems. SOPs assume staff have undertaken the mandatory clinical system training and are aligned to trust policies and processes, which set out the minimum Trust expectation. All services should be working to a SOP.

- SOP implementation and maintenance is the responsibility of the service(s) they pertain to. Support for this process can be co-ordinated by business teams.

- SOPs should be reviewed annually by the service as a minimum or as part of patient pathway/ service changes as well as during clinical system changes.
- It is important SOPs are maintained and adhered to and fully reflects the patient pathway.
- Issues identified through SOP review impacting data quality must be reported to the Data Quality Committee through data quality monitoring reports.

7.2 System Change (optimisation)

All requested changes to clinical systems must be made through the single change control process. These changes must be agreed by all relevant stakeholders prior to implementation and documented appropriately.
System changes must be considered against local and national reporting requirements, clinical safety and information governance requirements

System changes must comply with national standards to ensure that the Trust remains compliant with nationally mandated information standards

7.3 Data Entry

All staff entering data onto any clinical system must receive formal training at local induction before access is provided. User guides for clinical systems are available via Staffnet. The minimum data entry quality requirements are set out below:

- Staff must use standardised, rigorous searches on registration screens in order to identify patients accurately (including spine matching with the patient demographic service);

- The Trust encourages services to talk to patients to check and update their key demographic details to enable accurate recording on clinical systems i.e. at first contact with the patient and then to routinely check the information remains correct;
- The patient NHS number, date of birth, gender, ethnicity, current address (including postcode) and GP practice must be recorded;
- The Trust considers the most efficient way of maintaining quality patient records is to ensure that data items are correct at the point of recording:
- Data collected is reviewed at the time of first contact with the patient to ensure that all core data items are accurately recorded. Information must be validated with the patient at the first and subsequent contacts.
    - This should be done as soon as possible after the patient is seen or when the procedure is complete - This should be no later than the end of the shift on inpatient areas; or no later than 24 hours after the event in community based services.
- Where data is recorded inaccurately or incompletely, it is the responsibility of the service recording the data to make corrections. Where possible this should be completed by the individual responsible or where this is not possible another member of the care team with appropriate professional registration. This extends to data which has been recorded incorrectly in the past to ensure that data within the clinical record is fit for purpose and maintains the integrity of the clinical record.
- Where on-going and regular issues with data collection are identified, these should be fed into the development of training/ update programmes and escalated as a risk as appropriate to the Data Quality Committee by the Directorate representative or by any stakeholder to this policy.

7.4 Data Validation

All staff entering data are responsible for the quality of the information they enter onto clinical systems.

Services are required to implement and enforce robust data validation processes to ensure the quality of data held in clinical systems. These include but are not limited to:

- weekly patient tracking lists
- weekly caseload cleansing,
- weekly patient outcome measure (POM) reviews,
- annual record keeping audits etc.

Wherever possible, reports for data validation should be extracted directly from the clinical system.

Issues relating to any of the six domains of data quality identified during data validation should be recorded and action taken locally to resolved and reported to Data Quality Committee.

Local support for actions can be sought from the directorate Business Manager, Clinical Safety Officer (CSO), LHIS Change Manager or relevant Business Information Manager. Actions which cannot be resolved locally should be escalated to the Head of Service and Clinical Coding Assurance and Data Quality Manager.

If the issue affects the performance of a national or contractual information, the Head of Service should flag this with the Head of Information immediately. The Head of Information is responsible for assessing the risk from a Trust performance perspective and escalating

to the Senior Information Risk Officer (SIRO) as necessary.

7.5 Data Warehouse

The data warehouse provides a single source of patient information and activity by consolidating information from all the trust's clinical systems.

- The data warehouse **should** be used for management and performance reporting.

- The data warehouse **should not** be used for operational or clinical decision making.

7.6 Information Delivery

All regular reports will be supported by technical standard operating processes (SOP), which clearly determines how and when information is extracted from the data warehouse (or otherwise) and is used to populate reports.

Known technical issues affecting performance will be documented within the reports as supporting information. Where issues are persistent these should be reported through to the Data Quality Committee for review.

7.7 Performance Review, Authorisation and Submission

Services are required to quality assure the management and performance reports provided to them. The performance review should consider both the operational performance of the service as well as the quality of the data from which the performance measure is derived.

The quality of the data will be measured using Directorate Highlight reports to the Data Quality Committee bi-monthly. These reports will ensure that the elements outlined in the Data Quality Action Plan outlined in Section 7 of the policy are being addressed within directorates and that appropriate assurance controls are in place.

Directors of Services are required to authorise the release of information to external/ public bodies including but not limited to trust board, commissioners, NHS Digital, CQC etc. Information shall not be released externally unless it has received explicit consent to do so.

This authorisation will confirm that the relevant authority has deemed the information reported to be (see introduction for details):

- Reliable
- Valid
- Timely
- Complete
- Accurate
- Relevant

Consideration should be taken to caveat/ pause submission of national reports where significant data quality issues have been escalated to the Senior Information Risk Owner (SIRO). Agreements to caveat or pause national submissions must be endorsed by the Finance and Performance Committee (FPC) and noted at Trust Board.

7.8 Collection and Use of the NHS Number

The NHS Number is the mandated national unique identifier for patients and must be used alongside other demographic information to identify and link the correct records to a particular patient.

Everyone registered with the NHS is England and Wales has their own unique NHS Number. Patients who have not registered with a GP practice will not have a number. Overseas visitors may have been issued with a temporary number and people who are not eligible for free NHS treatment can have an NHS Number. Babies born in England and Wales are issued with NHS Numbers soon after birth. All correspondence, both paper and electronic, must include the NHS Number.

Frontline staff must ensure the NHS number is collected at the earliest contact of the patient with the trust. Every effort must be made to improve completeness and accuracy through real-time and on-going tracing and validation.

Batch tracing of patient data will be undertaken by LHIS to maximise the coverage of NHS Numbers in the patient master index for patients who have recently attended the trust. Resulting data quality reports are followed up by the frontline staff to ensure that completion is as high as practically possible.

8 Data Quality Plan

The Data Quality Plan is a key document and forms the work plan sitting under this policy. The plan is owned and managed by the Data Quality Committee on behalf of the Trust. The Action Plan forms the work programme for the year and requires all stakeholders to actively support on the delivery of agreed objectives to enable improvements in Trust data quality and compliance with local and national requirements.

9 National Data Sets

LPT is required to submit national data sets including but not limited to mental health (MHSDS), community services (CSDS) and Commissioning Data Sets (CDS) to the Secondary Uses Service (SUS) to:

- Provide data at patient level to commissioners of activity;
- Fulfil the requirement for compilation of Hospital Episode Statistics (HES) by the Department of Health and Social Care (DHSC);
- To meet data quality standards included within the Care Quality Commission Health check – e.g. coverage of ethnicity data and the quality of maternity and births data.

In order to meet the requirement to submit national data sets the Trust needs to ensure that it remains compliant with all current and future information standard notice releases. This ensures that data is being coded appropriately and that data can be easily provided to support patient treatment and to support accurate and timely reporting,

10 Data Pseudonymisation and Anonymisation

Patient identifiers such as name and address are required to be removed from CDS when the patient's NHS Number is present. The Human Fertilisation and Embryology Act 1990 as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992 impose statutory restrictions on the disclosure of information about identifiable individuals in connection with certain infertility treatments. The trust therefore omits all patient identifiers from CDS where required, and also where it has additionally chosen to do so.

11 Training needs

Achieving and maintaining good data quality requires on-going education and training throughout LPT. No staff members must be able to use or enter data onto key patient information systems, without adequate training. This includes temporary, locum and clinical staff.

The training programme must cover all aspects of information quality required:

- The definition of individual data items - so staff know what they are recording.
- The function of data – so staff know why they are recording data.
- How to validate data with the patient or against the records – so staff are recording the correct data.
- The correction of errors – so staff know how to correct errors and how to report errors if they find them.

The eventual use of data – so staff understand what the data they are recording will eventually to be used for and therefore why it is important to get right.

All staff should receive training and awareness sessions to ensure that they understand the importance of accurate patient identification to minimise clinical and organisational risk. As a minimum, the combination of LHIS clinical system training and the service specific Standard Operating Process (SOP) will cover these requirements.

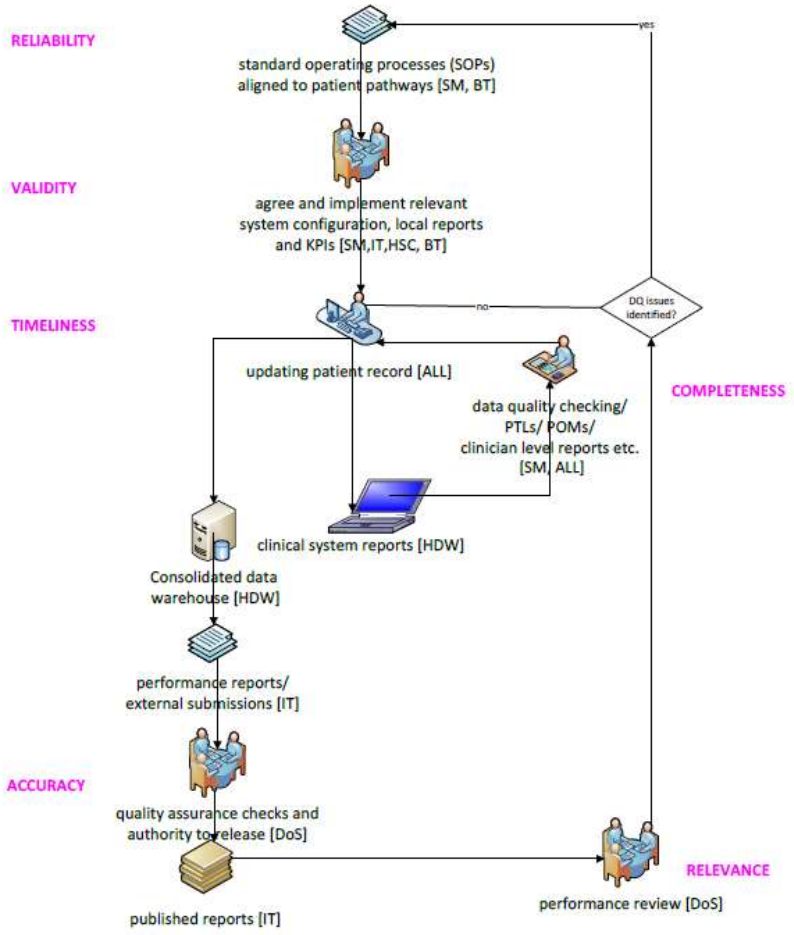
12 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
Section 5	Meeting the national quality standards for data completeness	Services are collecting and recording appropriate patient information on the clinical information systems	Data quality feedback through standard reports	Data Quality Committee	Bi-Monthly

Section 5	Annual review of themes and issues	Audit outcomes	Agenda and minutes of Data Quality Committee	Data Quality Leads reporting to Data Quality Committee	Annually

13 Flowchart/Process Chart

Key:
[DoS] Director of Service
[HoS] Head of Service
[SM] Service Manager/ Team Lead
[BT] Business Teams
[ALL] All Staff
[IT] Information Team
[HSC] HIS System Change Team
[HDW] HIS Data Warehouse Team



14 Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Sarah Ratcliffe	Head of Data Privacy/ Group Data Protection Officer
Hannah Plowright	Data Privacy and Information Governance Manager/Deputy Data Protection Officer
Prakash Patel	Head of Information
Usha Odedra-Parmar	Data Privacy and Information Security Manager

Circulated to the following individuals for comment

Name	Designation
Data Quality Committee	Group includes (in addition to the above): Director of Finance and Performance, Chief Clinical Information Officer, Business Information Managers, Clinical Safety Officer, Clinical Coding Assurance and Data Quality Manager, Directorate Business Team representatives, Clinical Systems Change Manager, Risk Manager.
Policy Group	

14 Links to Standards/Performance Indicators

Key Performance Indicator	Target/ Standards
Data Quality Maturity Index (DQMI) – Mental Health Services Data Set score	>= 95%

15 References and Bibliography

The policy was drafted with reference to the following:

- National Audit Commission's framework 'Standards for Better Quality Data' (Nov-2007) Retrieved from: https://webarchive.nationalarchives.gov.uk/20080806164253/http://www.au dit-commission.gov.uk/Products/NATIONAL-REPORT/AE298947-73F0- 4dcb-AF77-D2520EECBCFB/ImprovingInformationToSupportDecisionMaking.pdf
- NHS Oversight Framework (23-Aug-2019) Retrieved from: https://improvement.nhs.uk/resources/nhs-oversight-framework-201920/

This policy was drafted with reference to the following policies:

- Data Protection and Information Sharing Policy
- Information Lifecycle and Records Management Policy
- Electronic Health Record Policy (including record keeping and management)
- Patient Information Policy

Appendix 1

The NHS Constitution

Complete the Check List in order to provide evidence that you have considered the principles of the NHS Constitution. For further details please refer to the Development of Procedural Documents Policy

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 2

Due Regard Screening Template

Section 1	
Name of activity/proposal	Data Quality Policy
Date Screening commenced	September 2022
Directorate / Service carrying out the assessment	Information Service
Name and role of person undertaking this Due Regard (Equality Analysis)	Prakash Patel –Head of Information
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The aim of this document is to identify the intentions of Leicestershire Partnership NHS Trust (LPT) in assuring the quality of information which supports its business. Specifically that is: • Information that enables effective and timely communication regarding patients and care; Information upon which the Board relies to monitor and manage LPT's performance in all aspects of its business which is included in the performance reports.	
OBJECTIVES: To improve and monitor clinical system data quality	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	No impact
Disability	No impact
Gender reassignment	No impact
Marriage & Civil Partnership	No impact
Pregnancy & Maternity	No impact
Race	No impact
Religion and Belief	No impact
Sex	No impact
Sexual Orientation	No impact
Other equality groups?	No impact

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 is a neutral policy with no positive/ negative impact on any specific group			
Signed by reviewer/assessor	Prakash Patel	**Date**	01/06/2023
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed	Prakash Patel	**Date**	01/06/2023

Appendix 3

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:	**Data Quality Policy**		
Completed by:	**Sarah Ratcliffe**		
Job title	**Head of Data Privacy/Group Data Protection Officer**		**Date 02/06/2023**
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@.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:	**Sarah Ratcliffe**
Date of approval	**Date 02/06/2023**