University Hospitals of Leicester NHS
NHS Trust

Information Quality Policy

Approved By:	**UHL TRUST EXECUTIVE**
Date of Original Approval:	**11 December 2003**
Trust Reference:	B18/2003
Version:	**V7**
Supersedes:	**V6 December 2019**
Trust Lead:	Shirley Priestnall – Head of Information, Operations Directorate
Lead Board Director	Jon Melbourne, Chief Operating Officer
Latest Review Date:	**19 May 2023 – Policy and Guideline Committee**
Next Review Date:	**October 2026**

CONTENTS

Review date and Details of changes made during review April 2023:

- Data Quality Forum is renamed as Data Quality Assurance Group throughout
- The Chief Information Officer is now the chair of the DQAG.
- The Data Quality Assurance Group process is now that the relevant Trust Executive Director, signs off the assessment after it has been presented at the DQAG rather than before.
- Clinical Coding manager – clarify that responsibility is primarily for coding of admitted patient activity.
- Emergency & Specialist Medicine Clinical Management Group – has responsibility for coding of Emergency Care Data Sets.
- Data Quality Team – expanded explanation of responsibilities
- There is now a Datix incident category for “Incomplete/inaccurate information” for use by all staff
- Terms of Reference of the Trust’s Data Quality Assurance Group removed due to annual review timeframe

KEY WORDS

Data Quality, Information, Commissioning Data Sets, CDS, Performance, Assurance, Assessment, Diamond, DQAG, Assurance Framework, NHS Number

1 INTRODUCTION AND OVERVIEW

1.1 This document sets out the University Hospitals of Leicester (UHL) NHS Trust policy for ensuring that high quality data is collected about patients and activities undertaken by the Trust. Robust information is required for the delivery of better and safe patient care. It supports the delivery of core business objectives, research and to monitor performance. A vital pre-requisite to the production of reliable information is high quality data processing across all areas of the Trust.

1.2 The Data Protection Act of 2016 also sets the legal requirement for data users to ensure that personal data is kept accurate and up-to-data as one of its fundamental underlying principles.

1.3 Following recommendations from the Public Inquiry into Mid-Staffordshire NHS Foundation Trust, the Department of Health has introduced legislation. Where a provider is found to have published or provided information that is false or misleading in a material respect this is a criminal strict liability offence. The regulations apply to information from which data on mortality is derived and which may result in harm to patients if provided in a false or misleading way. The regulations also apply to Quality Accounts.

1.4 This policy lays out the intentions of the Trust to assure the quality of patient and activity information. Data that is proven to be of high quality supports effective and efficient patient care and accurate assessment of performance.

1.5 The policy promotes information quality such that:

a) The Trust can deliver safe patient care using accurate and timely data (Clinical risk is minimised).

b) Clinical governance is adhered to, and accurate data is available to identify areas for improving clinical care;

c) Administrative processes provide efficient means of communicating with patients and carers.

d) Reliable information is used to report the Trust's performance to the Board and stakeholders.

e) Planning of future services can be undertaken with confidence.

f) The Trust can reliably measure its own performance and compare that with peers and national trends.

g) The Trust can provide robust data for both feasibility and capability assessments for potential research opportunities.

h) The Trust can ensure that it is compliant with the Research Governance Framework, the EU Directive Medicines for Human Use (clinical trials) 2004 and subsequent related legislation, regulations, and frameworks.

2 POLICY SCOPE

2.1 This Policy applies to all UHL staff, including bank and contract staff, who collect and/or process patient, activity, or performance information.

2.2 The standards in this policy relate to data for all patients who are referred to the Trust for care and to all staff data as applicable.

2.3 The standards apply to:

(i) data held on computers or other media e.g., paper, film, tape.

(ii) data that forms any part of the Trust's Performance and Quality reporting mechanism (including non-clinical systems e.g., Electronic Staff Record System)

(iii) All information systems that are owned, used, or managed in the Trust

3 DEFINITIONS

3.1 Accuracy

Data is assessed to be accurate when:

- It reflects what actually happened.
- Data collection is supported by the availability of validated and regularly updated procedures and local reference tables.
- Opportunities are taken to ensure data accuracy e.g., checking information with the patient.

If data is found to be inaccurate, suitable remedial actions must be agreed between data collectors and validators. Improvement in accuracy, depending on the cause, must be achieved within appropriate time-frames.

3.2 Completeness and Coverage

Data is assessed to be complete when:

- All required data is collected.
- Data reflects all work done.
- Electronic records are an accurate reflection of manual records and required data items cannot be by-passed.
- Default codes are used where appropriate and not to cover missing data.
- For patient level data collection, the NHS Number is used in all identifiable references to patients. This is also supplemented by the local System Number since not all patients at the Trust have an NHS Number

3.3 Payment by Results (PbR)

Payment by Results is a reimbursement mechanism for acute care payments. It is a rules-based payment system which uses the complexity of the patient's healthcare needs to pay the provider for each patient treated.

3.4 Relevance

Data is assessed to be relevant when:

- It is collected for specific purposes.
- Staff have an understanding of the purposes for which the data is used.
- Requirements are periodically reviewed to ensure changing needs are accommodated.

3.5 Reliability and consistency

Data is assessed as reliable or consistent when:

- Relationships between data items are correct e.g., sequential and in correct context.
- Staff have procedures to follow, and data collection is not subject to personal interpretation.

- Computer systems used have validation rules configured to minimise the entry of conflicting data.

Proof that data is reliable and consistent ensures that progress towards performance improvements reflect real changes rather than variations in data collection

3.6 **Secondary Uses Service (SUS)**

The Secondary Uses Service (SUS) is national data supporting the NHS and its partners by providing a single source of comprehensive patient activity data. This anonymised patient-based data is used for planning, commissioning, management, research, audit, public health, and performance monitoring.

3.7 **Timeliness**

Data is assessed to be timely when:

- It is collected quickly and meets contextual deadlines.
- For patient care, data is collected as near to real-time as possible.

Timely data recording has the benefit of making information widely available to all relevant parties. Timeliness may take priority over accuracy in the short term for urgent treatment of patients

3.8 **Validity**

Data is assessed to be valid when:

- Rules and definitions are correctly applied.
- Computer systems used are configured to accept only valid codes and information is collected according to a pre-defined code-set.
- Codes collected comply with national NHS Standards (where they exist) and where local (e.g., Trust specific) codes or categories are used, these can be mapped to distinct national categories.

4 ROLES AND RESPONSIBILITIES

4.1. Executive Responsibility

The Chief Operating Officer has responsibility for application of this policy.

4.2. Executive Board

The Executive Board receives quarterly reports from the Head of Information on the Trust's commissioning information quality.

4.3. Deputy Director of Quality Assurance

Responsible for the production of the Trust's Quality Account.

4.4. Chief Information Officer

Chair the Data Quality Assurance Group

4.5. Trust Data Quality Assurance Group

4.5.1. This assurance group exists to make assessment of the quality of data reported to the Trust Board and to external agencies to ensure that it is of suitably high quality, is timely and accurate

4.5.2. Where such assessments identify shortfalls in data quality, the assurance group will identify risks and make recommendation for improvements to ensure that the quality is raised to the required standards

4.5.3. The group will use the locally agreed controls assurance process to review existing data systems and processes and provide scrutiny and challenge on the quality of data presented.

4.5.4. Advice and direction will be offered to Clinical Management Groups (CMG) and corporate teams on how to improve the quality of their data

4.6. Clinical Management Group (CMG) and Corporate Directors and Managers

4.6.1. Accountable for ensuring compliance with the standards documented in this Policy and related Procedures to ensure that data processing is of a high standard.

4.6.2. Accountable for the completeness and integrity of the data which is recorded within their CMG or Corporate Directorate.

4.7. Head of Information

4.7.1. Assure the quality of the Trust's Commissioning Data Sets submitted to the Secondary Uses Service (SUS), to standards defined by the Data Security and Protection Toolkit and as required by commissioners. Ensure that data is submitted to SUS within national timeframes.

4.7.2. Feedback to CMGs where data inaccuracies occur and where data entry or correction is not occurring in a timely manner.

4.7.3. Identify problems (through regular checks and audits) in the Trust's data processing which will impact information quality and where necessary facilitate correction.

4.7.4. Provide advice on good data management practices.

4.7.5. Ensure that changes required by external agencies for data provided by the Trust are actioned in a timely and consistent manner (e.g., Information Standards Notices);

4.7.6. Ensure the provision of management information on data quality, sourced from the Trust data warehouse as necessary.

4.7.7. Develop audit programmes to establish the integrity of the data, conducting audits and reporting the results of those audits to CMGs and the Executive Board.

4.7.8. Co-ordinate the activities of the Data Quality Assurance Group.

4.7.9. Advise CMGs and Corporate Directorates on the requirements for compliance with the local Data Quality assessment process.

4.8. Data Owner (within the Data Quality Assurance Framework)

4.8.1. This is the individual who is responsible for completion of the Data Quality Assessment for a specific indicator

4.8.2. Complete the Assessment Proforma accurately and in sufficient detail to enable the Data Quality Assurance Group to assess the data processing for the indicator.

4.8.3. Where applicable, accumulate process descriptions and assessment information from other individuals or departments who have an impact on the quality of data collected

4.8.4. Attend the Data Quality Assurance Group to present the assessment and respond to queries.

4.8.5. Undertake or co-ordinate improvements to the assessment as required by the Data Quality Assurance Group

4.8.6. If lack of assurance is identified for any of the data quality components, facilitate specific action plans within agreed timeframes. Support the Data Quality Assurance Group with information for re-assessment as necessary

4.9. Computer System Leads/Managers

Each of the Trust's computer data collection systems has a named role with responsibility for the quality of data on those systems. These will be named in the Trust's Asset Register.

4.10. Data Quality Team

4.10.1. Chair Corporate Data Quality Meetings held with administrative leads from each CMG, to ensure error reports are prioritised and remedial action taken. Provide detailed advice to resolve data quality concerns.

4.10.2. Daily checking of new electronic patient registrations (on HISS/PatientCentre) are undertaken to identify and resolve possible duplicate patient records.

4.10.3. Review patients where identification is not clear to ensure that NHS Number coverage is maximised, and potential overseas patients are identified. This includes routine identification of duplicate patient electronic records and ensuring the quality of new registrations.

4.10.4. Resolve records involving erroneous merging of records and support redaction activities within patient records

4.10.5. Sponsor other staff for access to the Summary Care Record for validating patient demographic information.

4.10.6. Use external systems to validate patients GP registration recorded and make amendments as necessary. This is vital for commissioning of services, since commissioners may withhold payment for activity attributed to the wrong practice.

4.10.7. Ensure all known patient deaths are recorded at the earliest opportunity.

4.10.8. Use Internal and External Data Quality reports to drive improvement. Use benchmarking data to review data quality and ensure high standards are achieved.

4.11. Clinical Coding Manager

4.11.1. Accountable for the accuracy and timeliness of the clinical coding data for admitted patients which is recorded on the HISS/PatientCentre. Clinical coding will be 100% complete by 15 calendar days following the month end in which the activity occurred.

4.11.2. Provides advice on applicable procedure codes for use in outpatient settings. Outpatient procedures are documented by the clinician (on outcome sheets) and entered into the Patient Administration System (HISS) by clinic co-ordinators.

4.11.3. Responsible for developing the audit programme to determine the quality of the clinical coding undertaken.

4.11.4. Responsible for arranging external audits of clinically coded data.

4.11.5. Manage the Clinical Coding Team.

4.12. Emergency and Specialist Medicine CMG

Coding activities undertaken with the Emergency Department (for the Emergency Care Dataset ECDS) are the responsibility of the CMG.

4.13. CMG and Corporate Directorate Managers

4.13.1. Critically appraise production of their own performance data and manage improvements required.

4.13.2. Accountable for the correction of errors and responsible for promoting good data management practices and providing necessary support.

4.13.3. Facilitate training where required and ensure that competency in use of electronic systems features as an element of performance appraisal for relevant staff.

4.13.4. Manage the effectiveness of arrangements for updating local documentation as data standards develop (national and local changes)

4.13.5. Ensure that sufficient front-line staff who register new patients have access to Summary Care Record via the NHS Spine Portal (NHS Smartcard access). This must be used to validate new patient records and obtain correct NHS Number and GP information.

4.14. UHL Researchers

Researchers must ensure that Trust policies, the Research Governance Framework and the Principles of Good Clinical Practice are followed.

4.15. Data collectors (administration, management and clinical staff)

4.15.1. Data collectors and entrants are responsible for the completeness and integrity of the data they record. Data must be recorded within agreed local timescales.

4.15.2. Accurate data collection is the responsibility of clinical as well as administrative and clerical staff. Although clinicians and nursing staff are frequently not traditional "data collectors" they do collect rich data on various departmental systems.

4.15.3. Log incidents relating to "Incomplete/inaccurate information" on Datix and flag with this category. These incidents are then auto-forwarded to the Data Quality Team for information and for any required urgent actions.

5 POLICY STATEMENTS, STANDARDS AND PROCESSES

5.1 Reporting of Performance Data

Each service providing performance data on their activities is required to have a quality assurance process in place. In proportion to the complexity and scale of the data processed for each indicator, the following controls should be operational:

a) Regularly reviewed documented procedures are available to support the accurate capture, entry and validation of data.

b) Key processes and data checking procedures are documented, and a formal review programme is in place to ensure that key data and information is accurate.

c) Appropriate training is undertaken by staff in the correct use of manual or electronic systems for the production of information.

d) Records of quality arrangements and validation checks are retained for subsequent inspection for a minimum of 18 months (to allow for inspection);

e) Data capture systems and information production are risk assessed with risks recorded on the Trust risk register (Datix), in line with the Trust Risk Management Policy.

5.2 Data Quality Framework

The UHL Data Quality Framework has been developed as an assessment of data quality for key data submissions and performance indicators. It provides a level of assurance that the data reported can be relied upon to accurately describe the Trust's performance. The data sets and indicators to which it will be applied are set out in the Trust's Data Quality Assurance Group work plan.

5.2.1 Scope of the Data Quality Assurance Framework

The assessment applies to all Trust staff who have responsibility for submission of data detailed within the Data Quality Assurance Group's work plan.

For the assessment to be made, information about the data collection and processing must be provided by those with responsibility for the submission of the data, the 'data owner' and the Executive Director with lead responsibility.

The Data Quality assessment template must be completed and signed by the 'data owner'. This is submitted to the Data Quality Assurance Group for an assessment and rating of the data quality.

This should accumulate a picture of whether the data in question can be assured through evidence of effective controls in place. (Controls are objective checks undertaken to confirm or refute the data. They may be automated or manual, e.g. a system will only allow certain data to be entered, a report shows records for review, someone checks the data).

Once assessed by the Data Quality Assurance Group have made their assessment, sign off is required by the Trust Director who has lead responsibility for the indicator and will require assurance that necessary remedial actions are undertaken.

5.3 Quality Accounts

5.3.1 The Deputy Director of Quality Assurance is responsible for the production of the Trust's quality account each year.

5.3.2 Quality Accounts are published to set out how the Trust is improving quality. The account covers the Trust's performance in relation to patient safety, experience, and outcomes. It provides information on priorities for improvement and review quality performance. The Trust Board is required to declare their accountability for the content via Chief Executive sign-off.

5.4 Timely collection of data

5.4.1 Data about a patient will be 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 all subsequent contacts.

5.4.2 Until real time data can be collected, data is to be recorded within 15 minutes of activity having occurred. The Trust will aim for real time data recording in all locations where admissions, transfers and discharges occur.

5.4.3 Activity such as referral registration, outpatient clinic administration, waiting list addition should be recorded within 24 hours of notification.

5.5 Collection process

5.5.1 The Trust considers the most efficient way of maintaining information quality is to ensure that data items are correct at the point of recording. For example, staff must use standardised, rigorous searches on registration screens to identify patients accurately.

5.5.2 Appropriate responsibility for the accurate, complete, and timely entry of data into the Trust's computerised and manual systems rests with the individual who is recording that data.

5.5.3 Where it is found that any data has been recorded inaccurately or incompletely a pragmatic approach will be taken to data correction. Where errors are identified they should, where possible, be corrected by the individual responsible (if this information is available). Whatever solution is adopted, it remains the responsibility of the applicable CMG or Corporate Directorate recording the data to ensure its accuracy. Corrections to data entered incorrectly are to be undertaken as soon as possible after the error is identified. All errors must be corrected within 7 days, or have an action plan available stating remedial action.

5.5.4 Where ongoing and regular issues with data collection are identified, these must be fed into relevant training and update programmes. The Trust will also use this learning to inform future system development (electronic patient record) and data warehousing solutions.

5.6 Research data

5.6.1 In cases of research, data collection must also follow the European Directive Medicine for Human Use (Clinical Trials) 2004 and must comply with the Principles of Good Clinical Practice as set out on ICH GCP (Good Clinical Practice). To be compliant with principles 2.10 and 2.13 researchers will:

- Ensure that all clinical trial information is recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification.
- The implementation of systems with procedures that assure the quality of every aspect of the trial.

5.7 Documentation and Procedures

5.7.1 Data collection activities should be supported with the use of relevant procedure documentation. Local procedures should be disseminated appropriately and easily available for reference – the most up-to-date version as either a paper copy or electronically. If reliant on electronic copies, all relevant staff must have necessary access.

5.7.2 Documentation must contain the current and relevant definitions e.g., as contained in the NHS data Dictionary

5.7.3 Documentation and data processing should be updated in line with any new Information Standards Notices.

5.8 The NHS Number – find it, use it, share it

5.8.1 Frontline staff must ensure the NHS number is collected at the earliest possible point. The Personal Demographic Service (PDS) holds the Summary Care Record (SCR) which is the national database of NHS patient demographic details including name, address, date of birth, NHS Number and GP. This is available to staff via NHS Smartcard access. Service Managers should ensure that there is a good coverage of staff with access in order that data will be effectively checked.

5.8.2 Every effort is made to improve completeness and accuracy of NHS Number information through real-time and ongoing tracing and validation. A rolling program of NHS number validation is undertaken which compares a patient file sent from the Trust to data held on the PDS. The process automatically seeks to match patient details and then updates HISS/PatientCentre with the verification status.

5.8.3 The NHS Number is the mandated national unique identifier for patients and must be used alongside other demographic information to identify and safely link patient records. This was the subject of a National Patient Safety Alert in 2008 and 2009. All correspondence, case-notes, patient wristbands and patient care systems must include the NHS Number to support accuracy of identification. Patients will be encouraged to use their NHS number and it will be present on correspondence they receive.

5.8.4 Only IT Systems that support the principles of NHS Number use may be procured for use in the Trust.

5.9 Computer systems

5.9.1 The following standards apply to current key operational systems in the Trust such as Nervecentre, HISS/PatientCentre, Pathology (iLAB), Imaging (CRIS), Maternity (E3) and to the procurement of new systems which are used for the operational delivery and organisation of care. Retrospective audit systems are *excluded.*

5.9.2 Key operational systems must

a) Be as up-to-date as the organisation can reasonably make them.

b) Have built in validation programmes which are conformant with, or map to NHS Standards where these exist

c) Have master-file values that match NHS standard definitions, with no other values used unless these are mapped explicitly.

d) Have codes and validation programmes that are kept up-to-date and cannot be switched off or overridden by operational staff.

e) Be subject to regular audit to ensure that errors are identified and acted upon.

6 EDUCATION AND TRAINING FOR THIS POLICY

6.1 Staff must have the necessary access to key information systems in order to fulfil the requirements of this policy. Formal HISS/PatientCentre training is provided as part of induction and refresher training is available on request:

6.2 All corporate IT Training courses are booked via the Clinical Skills HELM on-line Booking System. For enquiries: Tel (258) 5662 Email it.training@uhl-tr.nhs.uk

6.3 Training guides for HISS/Patientcentre are available via the following link http://insite.xuhl-tr.nhs.uk/homepage/working-life/education--training/it-training/hiss-courses

6.4 For local departmental systems, local arrangements must be in place to ensure that all new staff are appropriately trained prior to use of the system.

7 PROCESS FOR MONITORING COMPLIANCE WITH THIS POLICY

The audit criteria for this policy and the process to be used for monitoring compliance are given in the table below:

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
Performance indicator assessment	Named data owner for each performance indicator	Completion of assessment forms.	Bi- annually (more often if processes change)	Named corporate lead for performance indicator to present to the Data Quality Assurance Group
Review of Data Quality assessment proforma	Data Quality Assurance Group (internal review)	Excel spreadsheet	Annually	Data Quality Assurance Group
Data Quality assessment	Data Quality Assurance Group	Completion of assessment forms. Log of checks and scores	Bi- annually (more often if processes change)	Data Quality Assurance Group to report to Executive Team every 6 months
Quality of patient administrative data collected	CMG Managers	Suite of data quality reports on Insite	Weekly	Key reports are reviewed at the weekly corporate waiting list meeting – Data Quality Service Manager and CMG Service Managers
Quality of data submitted to Secondary Use Service	Head of Information	Adherence to local processes and documentation	Weekly	Report issues Commissioner representatives at Commissioning meetings

8 EQUALITY IMPACT ASSESSMENT

The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 ASSOCIATED POLICIES AND SUPPORTING REFERENCES FOR THIS POLICY

9.1 Key Procedures fundamentally support the policy and are available as separate documents. Data collection guidelines, within the Procedures, are focussed on the requirements for generation of accurate and timely activity data. This applies on the community-wide HISS (Patient administration system) and diagnostic systems to support operational and administrative requirements.

9.2 Key related documents are:

- NHS Data Dictionary http://www.datadictionary.nhs.uk/
- Local Information Governance web pages http://insite.xuhl-tr.nhs.uk/homepage/working-life/managing-information/information-governance
- False or Misleading information offence: Guidance for Providers https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/403084/FOMI_Guidance.pdf
- Research Governance Framework http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4108962
- ICH Topic E 6 (R1) Guidelines for Good Clinical Practice (European Medicines Agency) http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500002874.pdf
- NHS Data Quality Assurance https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/data-quality

Local policies available on the Trust intranet in the Policy and Guideline Library:

- Personal Information Policy (B39/2007)
- Information Governance Policy (B4/2004)
- Corporate Records Management Policy (B25/2020)
- Confidentiality Audit Procedures & Policy (B10/2016)
- Data Protection and Confidentiality Policy (A6/2003)
- Access Policy for Elective Patient Care (B3/2004)
- Research Passport Policy (B1/2010)
- Checking Patient Demographic Details Guideline (B10/2014)

10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW OF THIS POLICY

10.1 This document will be uploaded onto SharePoint and available for access by Staff through INsite. It will be stored and archived through this system.

10.2 As a minimum, this Policy will be reviewed every three years by the Policy and Guideline Committee. It may be updated and reviewed more frequently to adopt any new recommendations at the forefront of best practice nationally.