CONTROLLED DOCUMENT

University Hospitals Birmingham
NHS Foundation Trust

# Informatics Data Quality Policy

| | |
|---|---|
| **CATEGORY:** | Policy |
| **CLASSIFICATION:** | Governance |
| **PURPOSE** | To detail the processes for Data Quality for Information Management |
| **Controlled Document Number:** | 574 |
| **Version Number:** | 5.1 |
| **Controlled Document Sponsor:** | Chief Strategy & Digital Officer (CSDO) |
| **Controlled Document Lead:** | Head of Health Informatics |
| **Approved By:** | Chief Executive |
| **On:** | 30th March 2022 |
| **Review Date:** | 30th March 2025 |
| **Distribution:**<br>• **Essential Reading for:**<br>• **Information for:** | All Staff who deal with patient data<br>All Staff |

## Contents



## Version Control

| Version | Title | Issue Date |
|---|---|---|
| 1 | Data Quality Policy | March 2010 |
| 2 | Data Quality Policy | 17/01/2011 |
| 3 | Data Quality Policy | 13/01/2014 |
| 4 | Informatics Data Quality Policy | 01/07/2019 |
| 4.1 | Informatics Data Quality Policy | 08/07/2020 |
| 4.2 | Informatics Data Quality Policy | 06/05/2021 |
| 5 | Informatics Data Quality Policy | 06/04/2022 |
| 5.1 | Informatics Data Quality Policy | 06/12/2023 |

## 1. Policy Statement

**1.1** This policy outlines University Hospitals Birmingham NHS Foundation Trust (the 'Trust') principles and framework for high quality patient data, recognised as an essential part of running a quality service and embedded in the organisation as a key priority for all staff. All reasonable measures will be taken to ensure that all patient information generated by the Trust is accurate, complete where appropriate, and created in real time.

**1.2** Data Quality is the term used to define and measure the completeness, accuracy, relevancy, accessibility and timeliness of all patient data generated by the Trust. The link below details these dimensions in more detail.
https://www.england.nhs.uk/data-services/validate/

**1.3** Accurate patient data is essential for:

- Clinical care delivery and patient safety
- Effective financial management
- Effective management of waiting times
- Effective demand and capacity management
- Accurate information for decision making and service improvement.
- The patient experience through high quality patient administration
- Quality Outcome Measures
- High quality research and innovation

**1.4** Inaccurate data and information can seriously impede performance improvement due to the inability to monitor and measure performance accurately when the data is suspect. This consequently may make effective decision making from analysis of the data difficult to achieve. An example of a key issue which may arise is that of whether or not a report is showing either poor performance, or poor data quality.

## 2. Scope

**2.1** This policy applies to all areas and activities of the Trust and to all individuals working for the Trust including bank & agency staff, contractors, volunteers, locum and agency staff and staff on honorary contracts.

**2.2** This policy will only be applicable to patient-derived data; staff-related data will be covered by separate quality processes by the Human Resources Department.

Data Quality policy relates only to data on systems for which the Health Informatics department has feeds into its data warehouse for and for data sets for which is has access.

The Data Quality policy relates only to data which meets either of the following criteria:

- It feeds into the Health Informatics Department (through a data warehouse)
- It forms part of a dataset which the Health Informatics department has access to

**2.3** This policy also excludes data obtained from Third Parties as the Trust is unable to control the quality of the data. Feedback will be provided to the data source if appropriate.

## 3. Definitions Table

| Definition | Explanation |
|---|---|
| CQMG | Clinical Quality Monitoring Group |
| CaPRI | Clinical & Professional Review of Incidents |
| IT | Information Technology |
| DQIG | Data Quality Issue Group |
| DQ | Data Quality |
| DSPT | Data Security Protection Toolkit |

## 4. Framework

4.1 All Trust systems, manual and electronic, containing internally generated patient data, will have the same level of scrutiny regarding the quality of the patient data they hold. Any issues with data quality will be reported by the Operational teams at the appropriate Governance structures IGG, SUAG & IGAG

4.2 The Informatics Data Quality Policy is to be read in conjunction with the Records Management Policy. Whilst the former aims to protect the quality of input and creation (i.e., accuracy and completeness) of corporate and patient data gathered by the Trust, the latter sets out a framework for effective information and records management within the Trust. The policy should also be read in conjunction with the Data Protection, Confidentiality and Disclosure Policy.

4.3 All staff should undergo system specific training before being given access to any Trust information systems. Individual Information Asset Owners (IAO) are responsible for identifying appropriate training for staff accessing Trust systems.

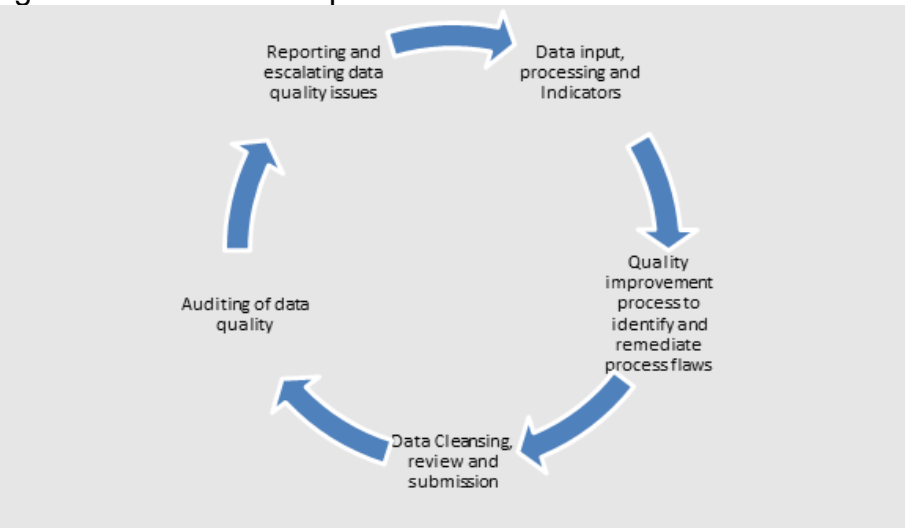
4.4 Data Quality is owned, monitored and managed through the line management structure, with issues raised and reviewed at the following forums:

- Clinical Quality Monitoring Group (CQMG)
- Information Governance Group (IGG)
- Clinical and Professional Review of Incidents (CaPRI)
- Data Quality Improvement Group (DQIG)

4.5 The Informatics Department will monitor the notices for all changes to national information standards. Any new information standards requiring changes to practice will be communicated to relevant staff at the earliest opportunity via email.

4.6 The Informatics Department will work closely with appropriate corporate services or clinical sites (primarily the Operational Performance Team) to routinely check for the validity and completeness of data used for national financial and activity monitoring processes, feeding any data quality process issues back to their source to aid continuous improvement.

4.7 The flowchart below shows the cycle for data validation and cleansing after inputting at source has taken place:




4.8 The Ward Clerk team leaders are required to undertake monthly quality monitoring checks of inpatient data entered onto Patient Administration System (PAS) by the Ward Clerks. A range of indicators are used to check

the accuracy of the inpatient data with the aim of achieving an accuracy rate of 95% or higher.

4.9 Data Quality Accuracy checks take place on specified fields in line with the Data Security & Protection Toolkit and reported to the Information Governance Group.

## 5. Data Quality Improvement Group (DQIG)

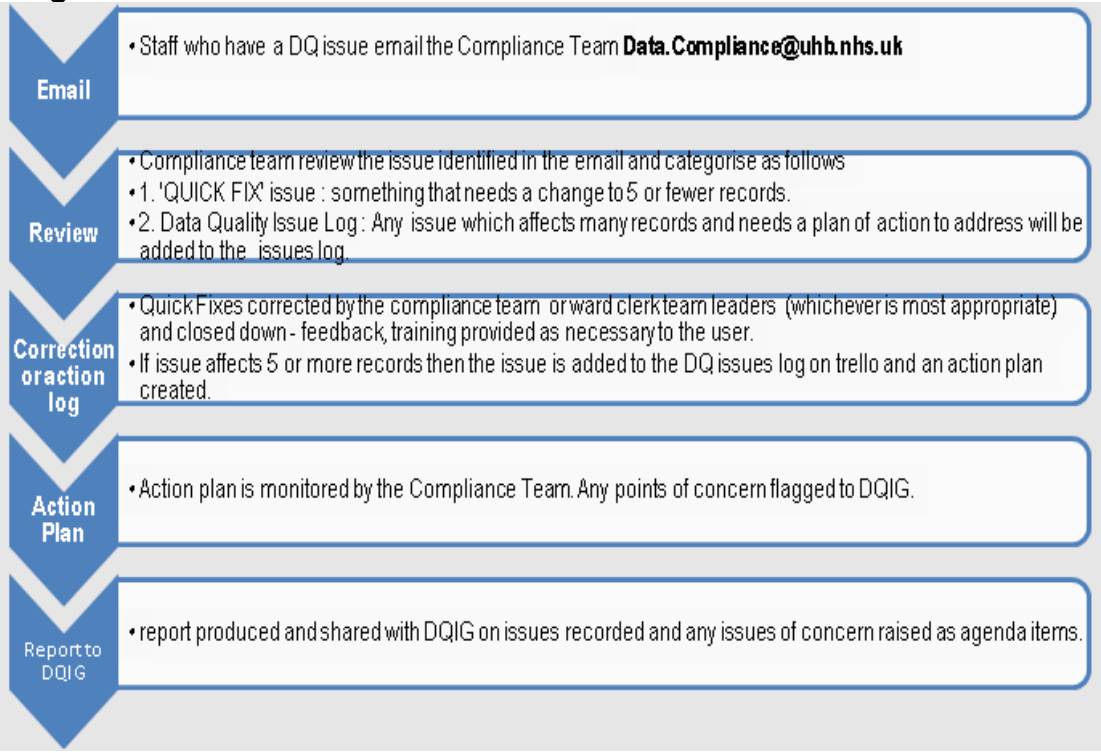
The Data Quality Issue Group is chaired by the Head of Health Informatics, meets monthly and reports outputs of the group formerly to the IGG on a quarterly basis. Any relevant issues are escalated to CQMG and DHG and the chair will also contribute and attend CaPRI upon request.

The report provides an update on the following:

1. The number of Data Quality issues documented on the Trusts Data Quality Issues log and on the new 'Quick Fix' issue log. Notification of new issues added, issues closed and any issues of concern.
2. Feedback & Actions from the Information Governance Group & sub groups.
3. DSPT
4. DQMI/UHB SUS Data Quality Dashboard
5. Update on the monthly Quality Monitoring Checks of Inpatient Data which are carried out by the ward clerk team(s).
6. Clinical Coding audits & Depth of coding
7. Feedback from West Midlands Data Quality Group
8. Actions Required – Next steps

A process for reporting DQ issues across the Trust has been established and is shown in **Diagram 1** below. An email address Data.Compliance@uhb.nhs.uk has been set up for Trust staff to flag data compliance/quality concerns to the Compliance Team.

**Diagram 1**




**5.1** Data Quality validations and accuracy checks take place against a range of quality indicators on all Trust activity using regular exception reports on a daily, weekly and monthly basis before submission to Secondary Uses Services (SUS), discrepancies are validated and corrected as appropriate. SUS is the single, comprehensive repository for healthcare data in England via NHS Digital. Any mandated returns submitted by the information team are signed off by the Head of the relevant departments the data applies to or a delegated equivalent.

**5.2 Peer** review takes place to check the accuracy and presentation of ad hoc requests.

**5.3 Individual** IAOs will ensure the monitoring and auditing of data in the information systems for which they are responsible. (See point 4.7)

## 6 Duties

### 6.1 Chief Strategy & Digital Officer

The CSDO has overall responsibility for ensuring appropriate mechanisms are in place to achieve and sustain high levels of data quality arising from corporate patient administration processes, IT

systems, training and medical staff and for the Information and Compliance teams.

### 6.2 Chief Operating Officer

The Chief Operating Officer has overall responsibility for managing performance with regards to site data quality and ensuring appropriate mechanisms are in place to facilitate recording and monitoring of accurate and complete data, so that quality is maintained at all times by the Sites with support from the Informatics department.

### 6.3 Chief Nurse

The Chief Nurse has overall responsibility for ensuring appropriate mechanisms are in place to enable all nursing staff to record accurate and complete patient data where appropriate.

### 6.4 Chief Medical Officer

The Chief Medical Officer has overall responsibility for ensuring appropriate mechanisms are in place to enable all staff within the Chief Medical Officers' portfolio are able to record accurate and complete patient data where appropriate.

### 6.5 Head of Informatics

The Head of Informatics has responsibility for ensuring effective processes are in place to monitor and report on levels of data quality, monitoring individual staff performance and highlighting areas requiring improvement and training.

### 6.6 Director of Patient Services

The Director of Patient Services has responsibility for ensuring effective processes are in place to achieve and sustain high levels of data quality in the following patient administration areas:

- Health Records Clerks
- Outpatient Clerks
- Booking Centre Clerks

### 6.7 Departmental Managers

All Departmental Managers are responsible for ensuring adherence to this policy, monitoring accuracy of patient data in their local systems. Departmental Managers are reminded that the duties set out in this policy are additional duties to those outlined in the Records Management and Information Lifecycle Policy.

### 6.8 Information Asset Owners

Information Asset Owners are responsible for ensuring that the appropriate processes are in place for maintaining the required standards for data quality, including staff training, monitoring and audit of data quality and the reporting of exceptions.

### 6.9 All Staff

All staff is responsible for the following:

- Ensuring they take appropriate care when recording, updating or validating patient information;
- Recognising the direct impact that incorrect information can have on patient care, raising concerns with their departmental managers when issues that may compromise the recording of accurate and timely information are identified.

## 7. Implementation and Monitoring

**Implementation**
This policy will be available on the Trust's Intranet and internet site. It will also be disseminated through the management structure within the Trust.
This policy will be implemented and monitored by the Head of Informatics. All staff members are responsible for data quality as outlined in this section; the Informatics Department will monitor staff competency following all training sessions.

**7.1** Implementation of this policy will take the form of effective individual staff performance measurement and monitoring through the line management structure in each department.

**7.2** The concept of Data Quality and its contributory role in the facilitation of effective patient care must be introduced to all new staff during local induction, as well as awareness to the Data Quality Policy.

**7.3** Data Quality will also be monitored externally by the use of The Data Security and Protection Toolkit through NHS Digital. This online system allows organisations to self-assess or be assessed against Information Governance policies and standards.

**7.4** Activity will be submitted monthly to NHS Digital, who provide a standardised data structure for providers to submit data into, named Secondary User Service (SUS). This tool promotes consistency and improved quality of data. The quality of data for the Trust is benchmarked nationally using the external SUS Benchmarking report.

**Monitoring**
Appendix A provides details on how the policy will be internally monitored by the Trust.

## 8. References

Data Protection Act 2018

Freedom of Information Act 2000

Computer Misuse Act 1990

NHS Data Model Dictionary for England

Data Security & Protection Toolkit (NHS Digital)

Data Sets Change Notification (DSCN) 31 and 32, 2008

## 9. Associated Policy and Procedural Documentation*

Reporting and Management of Incidents including Serious Incidents Policy

Procedure for the Reporting and Management of Incidents including Serious Incidents Requiring Investigation

Clinical Audit Procedure

Records Management (Corporate and Clinical) Policy

Data Protection, Confidentiality and Disclosure Policy

18 Weeks Referral to Treatment Guidance (Access Policy) (QEHB Only)

Appraisal and Archiving of Records

Medical Records Provision & Retrieval SOP (QEHB only)

Medical Records Pulling, Tracking SOP (HGS Only)

***Note: Pre-existing HGS controlled documents take effect as procedures where the UHB policy does not apply or are being updated and merged into a UHB document**

## Appendix A Monitoring Matrix

| MONITORING OF IMPLEMENTATION | MONITORING LEAD | REPORTED TO PERSON/GROUP | MONITORING PROCESS | MONITORING FREQUENCY |
|---|---|---|---|---|
| **Annual audits of Pseudonymised data**<br>The organisation has implemented an annual audit of a pseudonymised data requested from the Research and Development team to show the integration of data protection into processing activities.<br><br>DSPT - Evidence Ref **1.3.7** 2021/22 | Head of Programme Management & Compliance | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG) | Spot check audit of data within the Trust which has been pseudonymised.<br><br>An annual audit to takes place to identify a data request which has been pseudonymised. The audit checks that the technical controls in place have been carried out correctly.<br><br>An audit of data pseudonymised by the R&D team will take place & the results reported to the DQIG and then up to IGG. | Annual audit & report to DQIG and IGG. |
| **A data quality forum monitors the effectiveness of data quality assurance processes.**<br>The DQIG (Data Quality Improvement Group) meets monthly to review any DQ issues that have been flagged through the established processes for raising DQ issues within the Trust.<br><br>DSPT - Evidence Reference **1.1.8** 2021/22 | Head of Programme Management & Compliance | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG) | The Data Quality Improvement Group (DQIG) chaired by Head of Informatics meets monthly to review data quality issues which have been identified within the Trust.<br>Processes are in place for reporting and recoding data quality issues and these issues are logged on a central register and action plans are developed and monitored to ensure a process of continuous DQ improvement.<br>These processes are outlined within the DQ Policy (**see Section 7**) | DQIG meets Monthly & reports to IGG quarterly. |

| | | | | |
|---|---|---|---|---|
| **Data quality metrics and reports are used to assess and improve data quality.**<br><br>DSPT- Evidence Reference **1.1.7** 2021/22 | Head of Programme & Compliance Team (Health Informatics) | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG) | **Quality Monitoring Metrics**<br><br>Performance against defined quality monitoring metrics is monitored through the DQIG.<br><br>Ward Clerk team leaders carry out monthly quality monitoring checks of inpatient data entered onto the Trusts Patient Administration System (PAS) by the Ward Clerks<br><br>A range of key indicators are used to check the accuracy of the inpatient data with the aim of achieving an accuracy rate of **95%** or higher. | Monthly Quality Monitoring checks take place and are reported quarterly to IGG. |
| **Data quality metrics and reports are used to assess and improve data quality.**<br><br>DSPT- Evidence Reference **1.1.7** 2021/22 | Head of Programme & Compliance Team (Health Informatics) | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG)IGG | **Data Quality Maturity Index (DQMI)**<br><br>As part of the monthly reporting cycle to the DQIG the Compliance team review the published data quality metrics which can be found on the National Data Quality Maturity Index (DQMI)<br><br>Where an issue is identified an action plan is drawn up and monitored through DQIG.<br>The DQMI is available on the NHS digital website link below<br>https://digital.nhs.uk/data-and-information/data-tools-and- | Monthly |

| | | | | |
|---|---|---|---|---|
| | | | services/data-services/data-quality/data-quality-maturity-index-methodology | |
| **Data quality metrics and reports are used to assess and improve data quality.**<br><br>DSPT- Evidence Reference **1.1.7** 2021/22 | Head of Programme & Compliance Team (Health Informatics) | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG)IGG | **SUS (Secondary User Service)** Data Quality Dashboard reports.<br><br>As part of the monthly reporting cycle to the DQIG the Compliance team review the SUS dashboards reports for the Trust and report any areas of concern. Action plans to address any identified issues are drawn up and monitored through DQIG meetings.<br><br>All SUS DQ Dashboard reports can be found using the following link: \\nt0351_bdc_0003\I&C\CDS\checks\SUS_DQ\Source\202122 | Monthly |

| | | | | |
|---|---|---|---|---|
| Ensuring that patient records have the correct procedure and diagnosis codes recorded via Clinical Coding audit.<br><br>DSPT Evidence reference **1.1.7 metrics & reports** 2021/22 | Head of Programme & Compliance Team (Health Informatics) | Head of Health Informatics – Data Quality Improvement Group (DQIG) & Information Governance Group (IGG) | An annual audit of 200 FCES within the Organisation takes place against the Clinical Coding audit framework. This audit is completed by a qualified Clinical Coding auditor. Action plans against areas of non-compliance are created and monitored through the DQIG.<br><br>Formal audit reports are written.<br><br>There is also a programme of monthly audits of Clinical Coding as part of the department's clinical engagement and continuous improvement programme. | Annually |
| Health Informatics Department compliance with mandated Information Governance training.<br><br>DSPT Evidence reference **3.2.1** 2021/22<br><br>**Target** - Training compliance Trust target = at least 95% of all staff have completed their annual Data Security Awareness Training Local Health Informatics target = 90% | Senior Project & Business Analyst Manager | Information Governance Group (IGG)<br><br>Information Governance Assurance Group (IGAG) | Health Informatics compliance against mandated Information Governance training is monitored monthly by the Senior Project & Business Analyst Manager via reports sent through from the Easy Learning team.<br><br>These reports are shared with the Senior Management Teams within Health Informatics and compliance reported to DQIG, a report including IG training % compliance is presented to both IGG and IGAG. | Monthly reports to DQIG<br><br>Quarterly reports to IGG and IGAG. |

| | | | | |
|---|---|---|---|---|
| National Data Opt- out (NDOO)<br><br>Is your organisation compliant with the national data opt-out policy?<br><br>DSPT Evidence reference **1.2.4** 2021/22 | Head of Programme & Compliance Team (Health Informatics) | Information Governance Group (IGG) | A National Data opt -out SOP is in place and has been approved by Information Governance Group. A register of NDDO from HI department to be put in place and managed by the HI Compliance Team. (Note all submissions from HI are inclusive of NDOO and centrally applied by NHSD or DLP). | |