

Data Quality Policy

Version:	2.1
Approved by:	The Board
Date Approved:	29.11.16
Lead Manager:	Associate Director Quality and Governance
Consultation	Quality Assurance Board members, Assistant Director Information Governance and Data Security
Lead Director:	Director Quality
Date issued:	Nov 16
Review date:	Oct 21



Audit Trail		
Date	Changes made	Author
June 2020	<p>Section 6: Duties and responsibilities – updates to job and meeting titles and responsibilities. Addition of Student Data Analyst.</p> <p>Section 9: Process for monitoring compliance – updated to include details of the Quality Assurance Board</p> <p>General changes – IG Toolkit replaced with Data Protection and Security Toolkit and reference to student / educational returns</p>	<p>Marion Shipman, Associate Director Quality & Governance</p>

Contents

1	Introduction	4
2	Purpose	5
3	Scope	5
4	Definitions.....	5
5	Principles of Data Quality.....	5
6	Duties and Responsibilities	6
7	Procedure for data quality management	9
8	Training	9
9	Process for monitoring compliance with this policy.....	9
10	References.....	10
11	Associated documents	10
12	Data Pathways.....	11
13	Appendix: Equality Analysis for Policies and Procedures.....	12

Data Quality Policy

1 Introduction

The importance of having data of the highest quality on which to base its decisions, whether clinical, managerial, educational or financial, is recognised by the Trust. The importance of having robust systems, processes, data definitions and systems of validation in place to assure data quality is part of this process. The quality of data can affect the reputation of the Trust and may lead to financial penalty in certain circumstances, e.g. failing to meet contractual requirements such as Key Performance Indicators (KPIs), Commissioning for Quality and Innovation targets (CQUINs) and other reportable outcome measures.

The fourth data protection principle under the Data Protection Act 2018 is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

Complete and accurate data are essential to support effective decision making across the spectrum of Trust functions, including:

- Patient Care – in the delivery of effective, relevant and timely care, thereby minimising clinical risk.
- Good Clinical Governance – a pre-requisite for minimising clinical risk and avoiding clinical error and misjudgement.
- Disclosure – ensuring that clinical and administrative information provided to the patient and authorised health partners, including external partners is of the highest quality.
- Business planning – ensuring management can rely on the information to make informed and effective business decisions.
- The measurement of activity and performance to ensure effective distribution and use of Trust resources.
- Regulatory reporting – to ensure compliance with the standards and targets as laid down in measures such as CQUIN, Data Security & Protection (DSP) Toolkit, HESA student returns and Monitor Assessments.
- Good corporate governance – which, as above, has data quality as a pre-requisite to ensure effective business management.
- Legal compliance – ensuring that the Trust conforms to its legal obligations as laid down in relevant legislation, such as Data Protection Act.
- Education and Training – in the development and delivery of quality education and training provision and the effective administration of the student journey.

2 Purpose

The purpose of this policy, is to provide general principles for the management of all data and guidance. This is to ensure that the Trust can take decisions based on accurate and complete data and can meet its various legal and regulatory responsibilities.

3 Scope

This policy is applicable to:

- All data held and processed by the Trust.
- All data must be managed and held within a controlled environment and to a standard of accuracy and completeness. This applies to data regardless of format.

This policy must be applied by all permanent, contract or temporary staff, clinical and non-clinical and all third parties who process Trust data.

4 Definitions

Data quality is a measure of the difference between data collected on information systems or manually, against the true experience of the subject (eg for patient data), or the true occurrence of an event (e.g. for financial data).

Data validation is defined as systems and processes employed to verify the accuracy and completeness of data that is collected.

5 Principles of Data Quality

Data quality can be said to be 'high' if the data accurately portray exact details and/or events that actually took place. Measuring data quality can be vexatious and problematic, which is why the following principles should be considered when doing so.

5.1 Accessibility

Information can be accessed quickly and efficiently through the use of systematic and consistent management in electronic (and physical) format. Access must be appropriate so that only those with a lawful basis and legitimate relationship to the data may view, create or modify them.

5.2 Accuracy

Data (and information) are accurate with systems, processes and practice in place to ensure this. Any limitations on accuracy of data must be made clear to its users and effective margins of error need to be considered for calculations.

5.3 Completeness

Completeness can have a real impact on the quality of data. The evaluation of data quality must monitor for missing, incomplete or invalid information as well as identification of future or occurring causes and the associated risks.

5.4 Relevance

Data captured should be appropriate for the intended purpose and never excessive.

5.5 Reliability

Data and information must reflect a stable, systematic and consistent approach to enhance reliability. Review and enforcement of collection methods of data must be considered to ensure a positive impact on the quality or content of any information produced.

5.6 Timeliness

Data should be recorded as close as possible to being gathered and should be accessed quickly and efficiently, in line with the Data Protection Act.

5.7 Validity

Validity is supported by consistency over time, systems and measures; data must be collected, recorded and utilised to the standard set by relevant requirements or controls. Any information collection, use or analytical process must incorporate an agreed validation method or tool to ensure the standards and principles outlined above are met. Validation tools will support routine data entry and analysis, as well as supporting the identification and control of duplicate records and other errors.

6 Duties and Responsibilities

6.1 Chief Executive

The Chief Executive (CE) has overall responsibility for data quality systems and processes in the Trust. The CE is responsible for signing the statement of assurance of clinical data quality included in the annual Quality Report.

The responsibility for data quality is delegated through the Trust management structure, with specific responsibilities allocated as below.

6.2 Senior Information Risk Owner (SIRO)

The Trust's Senior Information Risk Owner (SIRO) is a director appointed by the Board of Directors (BD) who takes ownership of the organisation's information risk policy and acts as the advocate for information risk on the Board. The SIRO reports to the BD through the Integrated Governance Committee.

6.3 Finance Director

The Finance Director is responsible to the Board for assurance that systems and processes for finance data quality are in place and working effectively, and alerting the Executive Management Team (and the Board of Directors, if appropriate) of any significant risks to finance data quality.

6.4 Director of Quality

The Trust's Director of Quality is responsible to the Board for assurance that systems and processes for clinical data quality are in place and working effectively, and alerting the Executive Management Team (and the Board of Directors, if appropriate) of any significant risks to clinical data quality.

6.5 Associate Director of Quality and Governance

The Associate Director has operational responsibility for all clinical data quality reports. The Associate Director will liaise with internal and external stakeholders to streamline and reduce the collection burden wherever possible.

6.6 Assistant Director of IG & Data Security & Protection Officer

The AD IG and DSP has responsibility for the strategic and operational management of information governance, and for providing subject matter expertise in this area. The manager will assess quality of data related evidence submissions for the DSP toolkit submissions.

6.7 Clinical Governance and Quality Manager

The Clinical Governance and quality manager will lead on the management of data for clinical audit, patient safety and safeguarding, and will monitor clinical incident data for clinical risk and revalidation management purposes.

6.8 Quality Assurance Manager

The Quality Assurance Manager is responsible for providing guidance and support across a range of clinical data collection processes and advises on

Data Quality Policy, v2.1, June 2020

data quality improvements or changes necessary for reporting on the current and developing performance measures, such as CQUINs and KPIs.

6.9 Student Data Analyst

The Student Data Analyst is responsible for business processes relating to statutory student number returns, and updating relevant senior colleagues of any changes in statutory student number reporting.

6.10 Directors

Directors are responsible for the collation and validation of data in their respective directorates, alerting the Executive Management Committee (and the Board of Directors, if appropriate) of any significant risks to the data quality. Areas of responsibility are as follows:

Dataset	Data Quality Assurance Lead
Financial data	Director of Finance
IM&T data	Director of IM&T
Patient data (electronic and paper records)	Directors of CYAF Adult and Forensic and Gender services
HR records	Director of HR and Corporate Governance
Membership records data	Director of HR and Corporate Governance
Staff administration records	All Directors
Education and Training data	Director of DET

6.11 Managers

Managers are responsible for ensuring the quality of data within their teams, adhering to this policy and implementing the associated Data Quality Management Procedure.

6.12 Head of Informatics

The Head of Informatics is responsible for developing and validating reports based on commissioning and management requirements. The post holder also advises on tools and processes to monitor and measure the level of data quality within the Trust's electronic patient system. This responsibility extends to providing an early warning system of potential risks and actively monitoring and commenting on performance trends. The post holder works closely with the Quality Assurance Manager and Associate Director Contracts.

6.13 Chief Clinical Information Officer

The CCIO is a clinician responsible for developing information in support of better care. The CCIO will provide clinical and professional leadership to clinicians, informatics and the Quality Directorate to help ensure that the Trust delivers safe, effective, evidence-based and accessible services and systems

Data Quality Policy, v2.1, June 2020

to meet the health and care knowledge and information needs of patients and services users. The CCIO will also improve accountability and strengthen governance of the quality of the Trust's data by reviewing the Trust's performance in secondary use assurance.

6.14 Associate Director Contracts

The post holder is responsible for collating, validating and 'sense-checking' any data and information that will be reported to commissioners, as well as providing robust definitions and assurance of commissioning and reporting requirements. The post holder will also highlight any issues or concerns that are found through the reporting and validating processes, to the relevant Trust Directors.

6.15 All Staff

All staff have a responsibility to ensure the data they enter onto any system – electronic or manual is of good quality and follow Trust and local procedures for the validation of data.

7 Procedure for data quality management

Each director/manager listed in section 6 will publish procedures, or standard operating procedures, as indicated in order to discharge this policy in their domain.

8 Training

The importance of data quality will be included in:

- the Trust's mandatory training (INSET) and induction programme, as part of information governance and security training ;
- general CareNotes training offered by the Informatics department (clinical data), including outcome monitoring
- one to one Outcome Monitoring support provided by the Quality Assurance Team (clinical data);

Training issues with systems and/or other specific processes should be addressed on an individual basis as they arise.

9 Process for monitoring compliance with this policy

Data quality is ultimately the responsibility of department leads where the specific data are being generated. Processes for ensuring high data quality will differ between teams and should be implemented and reviewed locally.

Strategic oversight of clinical data quality is via the Quality Assurance Board (QAB). Operational oversight is via the Quality Assurance Team which provides information to the Quality Assurance Group (QAG) for review on a monthly basis. This group escalates issues of clinical data to the QAB. The Quality Assurance Board accountable to the Executive Management Team.

Assurance of management information systems, including assurance of data quality performance against the DSP toolkit standards, is considered by the Data Security & Protection Sub-Committee and reported to the Integrated Governance Committee (IGC) on a quarterly basis. The Associate Director of Quality and Governance provides evidence to the sub-committee to meet the specific data quality performance DSP toolkit requirements.

The IGC reports to the Board of Directors quarterly and flags clinical data quality risks via reports and via the operational risk register. The IGC also assures the quality of the draft Annual Quality Report in advance of external consultation and final presentation to the Board for approval.

Independent audit of all aspects of the Trust's business, including data quality are subject to periodic internal and external audit reviews. Findings and recommendations from these audits and subsequent action plans to address deficiencies are monitored by the Executive Management Team. These are overseen by the Audit Committee, which reports directly to the Board.

10 References

NHS Data Security Protection Toolkit: <https://www.dsptoolkit.nhs.uk/>

Gov.UK (2018), Data Protection Act, www.gov.uk/data-protection/the-data-protection-act

Data Protection Act (2018) <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

Information Governance Alliance (2016). Records Management Code of Practice for Health and Social Care. London:

11 Associated documents¹

This policy should also be considered in conjunction with all the policies and legislation, especially those highlighted below:

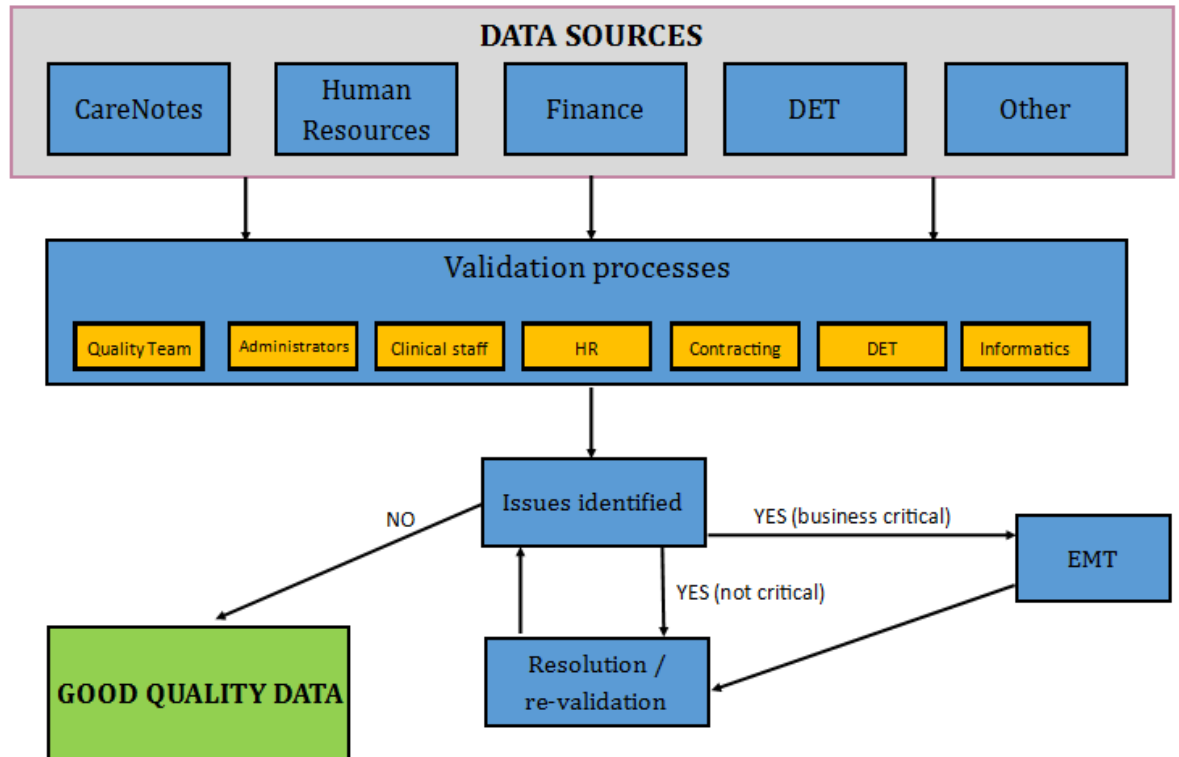
- Health records management procedure
- Health records audit procedure
- Confidentiality Code of Conduct
- Data Protection Procedure
- Information Asset Acceptance and Registration Procedure
- Information Governance Policy
- Risk Management Strategy and Policy
- Corporate and DET Records Procedure

¹ For the current version of Trust procedures, please refer to the intranet.

Data Quality Policy, v2.1, June 2020

12 Data Pathways

Diagram of data flows within the Trust with simplified validation and resolution procedures.



13 Appendix: Equality Analysis for Policies and Procedures

Completed by	Reviewed by Marion Shipman
Position	Associate Director Quality and Governance
Date	16 June 2020

The following questions determine whether analysis is needed	Yes	No
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the following analysis:

	Yes	No	Comment
Do policy outcomes and service take-up differ between people with different protected characteristics?		X	
What are the key findings of any engagement you have undertaken?			Wide consultation including Quality Assurance Group and Quality Assurance Board.
If there is a greater effect on one group, is that consistent with the policy aims?		X	
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?		X	

Will the policy deliver practical benefits for certain groups?		X	
Does the policy miss opportunities to advance equality of opportunity and foster good relations?		X	
Do other policies need to change to enable this policy to be effective?	X		Yes, Each director/manager listed in section 6 will need to publish procedures, or standard operating procedures, as indicated in order to discharge this policy in their domain.
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 – seek advice from Human Resources (for staff related policies) or the Trust’s Equalities Lead (for all other policies).