Data Quality Management Procedure

Version:	2.3
Bodies consulted:	Quality Assurance Board members, Data Security and Protection Manager and DPO and DET
Approved by:	EMT
Date Approved:	19 June 2020
Lead Manager:	Associate Director Quality and Governance
Responsible Director:	Medical Director
Date issued:	22 June 2020
Review date:	October 2024
Intranet?	Yes
Extranet?	Yes

Contents

Audit Trail		
Date	**Changes made**	**Author**
November 2018	Trust logo updated Title under section 5.5, 'Duties and responsibilities' updated Section 6.3.1 removal of reference to IGTK and information updated for meeting Data Security Standard 1.7.2. Section 6.4.3 updating information relating to the Clinical Data Quality Review Group Section 6.6 Additional section pertaining to information presented to Board on a quarterly basis. Section 7 Information Governance Toolkit information removed and reference to GDPR and DSPT Assertions added. Section 8 GDPR and DSPT Assertions reference added Appendix A Equality Analysis updated	Data Quality Manager
June 2020	**Amendment of title as 'Data Quality Management Procedure' (from Clinical Data Quality Management Procedure')** as Appendix B includes a specific 'Clinical Data Validation Plan' Section 5.5 'Duties and responsibilities' updated with job titles, Section 6.1 'Data Analysis Review Committee' replaced with 'Quality Assurance Board' Section 6.3.1 'Data Quality Assurance checks', updated to reflect annual documentation audits undertaken by services with support from the clinical governance team. Section 6.4 'Management arrangements for quality control', updated including renaming the Clinical Data Quality Review Group as the Quality Assurance Group, and the addition of the Quality Assurance Board to replace the Data Analysis Review Group (DARG). References and Associated documents update Appendix B 'Clinical Data Validation Plan' updated with job and group titles and to be moved from this procedure to the Health Records Management Procedure	Associate Director Quality and Governance

Data Quality Management Procedure

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.

Information accuracy is a legal requirement under the Data Protection Act 2018 and Public Records Act.

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

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

l. Research, including monitoring patient outcomes
m. Compare historical data and highlight trends
n. Monitor performance against key performance indicators and local and national targets

2 Purpose

This document sets out the procedures that need to be carried out to ensure good data quality management of the Trust's information.

It is important that data can be relied upon for its intended uses, including decision making and planning.

3 Scope

This procedure is applicable to all data held and processed by the Trust.

This procedure 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 (e.g. for patient data), or the true occurrence of an event (e.g. for financial data). High quality data is accurate, complete, relevant, reliable and timely.

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

5 Duties and responsibilities

5.1 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.

5.2 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.

5.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) acts as the advocate for information risk on the Board.

5.4 Director of Quality

The Trust's Director of Quality ~~and Patient Experience~~ 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.

5.5 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.

5.6 Chief Clinical Information Officer

The Chief Clinical Information Officer (CCIO) combines the expertise of a long-practicing medical clinician with the IT knowledge of a CIO role.

The CCIO will improve accountability and strengthen governance of the quality of the Trust's data by reviewing the Trust's performance in secondary use assurance.

5.7 Assistant Director of Information Governance and Data Security and Data Protection Officer (DPO)

The Assistant Director of Information Governance and Data Security & DPO has responsibility for the strategic and operational management of information governance, and for providing subject matter expertise in this area.

The postholder is responsible for ensuring the protection of personal data, that is, protecting the confidentiality, integrity and availability of personal data.

5.8 Clinical Governance Manager

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

5.9 Quality Assurance Manager

The Quality Assurance Manager provides guidance and support across a range of clinical data collection processes and advises on data quality improvements or changes necessary for reporting on the current and developing performance measures, such as CQUINs and KPIs. The individual is responsible for actively monitoring, commentating on and supporting staff to improve performance trends.

The post holder also has responsibility for the Quality Assurance Team, who undertake the completion and preparation of clinical quality based reporting for the Trust to ensure the robustness and validation of reportable data.

5.10 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
Education and Training data	Director of DET
Financial data	Director of Finance
HR records	Director of HR and Corporate Governance
IM&T data	Director of IM&T
Membership records data	Director of HR and Corporate Governance
Patient data (electronic and paper records)	Directors of CYAF, Adult and Forensic services, Gender Services and CCOO
Research records	Medical Director
Staff administration records	Respective Directors

5.11 Managers

Managers are responsible for ensuring the quality of data within their teams.

5.12 Informatics Manager

Informatics Manager is responsible for managing the reports development and validation processes for clinical and non-clinical systems and processes.

The role manages developers and senior analysts; who are directly involved in developing and validating reports, as part of the reports development process based on commissioning and management requirements. Requester and business and relevant service line is responsible for request validation and sign-off as new / change request process.

5.13 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 requirements for statutory student number reporting.

5.14 Associate Director Contracts

The post holder is responsible for '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.

5.15 Clinical Staff

Clinical staff have a responsibility to ensure the data they enter onto any system is of good quality and should undertake regular data validation checks.

5.16 Administrators (All services)

Administrators are responsible for following agreed local Standard Operating Procedures/checklists for the validation of data.

5.17 All Staff

Staff recording data either manually or electronically are responsible for ensuring that it is timely, accurate, and complete, complies with Trust procedures requirements, and that any error that is identified is rectified in the correct way.

In addition, staff members are responsible for following any local Standard Operating Procedures for the validation of data.

6 Procedures

The Trust has a number of interrelated processes to support high levels of data quality:

- Setting data standards
- Undertaking data validation

- Checking for and acting on missing or inconsistent data
- Managerial arrangements for quality control
- Standard Operating Procedures
- Reports and dashboards

6.1 Setting of data standards

Data standards ensure there is consistency in data collection by having agreed and implemented data definitions for key data items.

The Trust's Quality Assurance Board establishes data standards for key clinical data items and the directors under section 5.10 are responsible for establishing their own data standards. These may be externally mandated or best practice.

6.2 Undertaking data validation

Data validation should be undertaken using a variety of methods depending on the way in which the data are stored. The following should be taken at least on a monthly basis and will include:

- checking for the completeness of any data set and reviewing if missing information can be obtained and entered onto a system

- undertaking regular checks on service user and student data through rolling programmes of audit to check for completeness. For courses validated by university partners, student data will be shared on a rolling basis for validation purposes.

- validation of data entries

- checking any data output or report against the live system from whence it came to prove validity and accuracy

- 'Sense-checking' any information produced and comparing to similar or previous datasets

- Staff system training – no staff should be provided with editing rights until they have completed system training.

On a quarterly basis the following data validation should be undertaken where available:

- benchmarking, both local and national, to identify data quality issues and trends; any discrepancies should then be investigated

6.3 Checking and acting on missing or inconsistent data

Virtually all data systems are prone to inconsistencies. Any member of staff identifying inconsistency in data should either correct it (if in the scope of their role/responsibility) or draw it to the attention of an appropriate administrator or manager without delay. Errors and inconsistencies identified should be investigated and addressed by managers and escalated as appropriate e.g. to the Quality Assurance Team for clinical data.

6.3.1 Data Quality Assurance checks

These should be established by respective directors.

Clinical Data checks are run monthly by the Informatics department and the Quality Assurance Team, and followed up at the Quality Assurance Group via clinical governance representation, service leads and administrators, to improve data quality completeness and validity on carenotes data including reportable mandated fields (e.g. ethnicity, patient's postcode, outcome measures, care plans compliance rates, registered GP) to ensure that our data and submissions to NHS Digital are accurate, relevant and timely.

Clinical services undertake an annual case notes audit supported by the Clinical Governance Team to improve data accuracy and completeness and support compliance with new Data Security Standard 1.7.2.

6.4 Management arrangements for quality control

6.4.1 Team level

Day-to-day management of data quality lies with the respective team manager. Locally agreed procedures should be followed. .

6.4.2 Executive Management Team (EMT)

EMT will receive updates against key targets and standards from Data Quality Assurance Leads. EMT Members are responsible for reviewing and challenging any reported data that does not reflect their understanding of practice/outcomes, as well as commissioning data investigations and monitoring action plans.

6.4.3 Quality Assurance Group

This multidisciplinary operational group of clinical and senior administration staff meets monthly to analyse and - evaluate data from the patient administration system, identify key areas for improvement and take decisions to allow more accurate collection and reporting.

6.4.4 Quality Assurance Board

This group of Directors and senior managers meets quarterly and provides strategic oversight for data quality matters including review and sign off for the Board quarterly quality report.

6.5. Standard Operating Procedures (SOPs)

Local Standard Operating Procedures (SOPs) defining the processes required to accurately and effectively assure the quality of data should be agreed.

These SOPs should be reviewed on an annual basis, in conjunction with commissioning and management requirements, and adjusted where necessary to improve efficiencies in process and the quality of data collected.

6.6 Reports and dashboards

The Trust uses reports from a number of systems, which include SQL Server Reporting Services, and *CareNotes*.

Appropriate staff members have access and a responsibility to run, analyse and where appropriate, resolve issues identified on these reports.

A Quality Dashboard and Commentary report is presented to the Trust Board of Directors on a quarterly basis and includes key indicators from KPIs, CQUINs, MHSDS, Clinical Governance, HR and DET.

7 Process for monitoring compliance with this Procedure

There are several regular meetings in the organisation where data quality is reviewed, including the Quality Assurance Group and the Quality Assurance Board. Any deviation or noted change in data quality will be discussed at these meetings.

The Quality Assurance Team also monitors clinical data and information from *CareNotes* and more widely across the organisation and can be noted of any perceived data quality problems.

The Trust makes an annual submission against the NHS Data Security & Protection Toolkit (DSPT). Completion of the assertions relevant to data quality are the responsibility of the Associate Director of Quality and Governance.

Performance against the DSPT is monitored by the Data Security and Protection Sub-Committee of the Integrated Governance Committee.

8 References

Caldecott 2 Review 'To share or not to share' April 2013
A Guide to Confidentiality', NHS Digital, 2013
Caldecott 3 Review of Data Security, Consent and Opt-Outs, July 2016
Data Security and Protection for Health and Care Organisations, 2017/18
Department of Health
Confidentiality: NHS Code of Practice, DoH and Social Care, 2003
Data Handling Review, Cabinet Office, 2012
Data Quality Assurance Framework for Providers, NHS Digital, Jan 2020
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 Management Framework, v1.0, October 2018
Pages 16 of 18
Information Policy, DoH 2010
Information Security Management: NHS Code of Practice, Gov.UK, 2007
NHS Care Record Guarantee, National Information Governance Board for Health and Social Care, 2011
NHS Digital Data Security and Protection Toolkit, Information Commissioner's Office (https://ico.org.uk//)
NHS Information Risk Management, Digital Information Policy, DoH, 2009
Records Management Code of Practice for Health and Social Care, https://digital.nhs.uk/information-governance-alliance , 2016

9 Associated documents

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

- Acceptable Use Policy
- Access Control Procedures
- Code of conduct on confidentiality for employees
- Data protection procedure
- Health records management procedure
- Health records audit procedure
- Information asset acceptance and registration procedure
- Information governance and data security and protection management framework
- Information governance policy
- Information security policy
- Records retention schedule
- Risk management policy and strategy

Standard Operating Procedures may exist locally

Appendix A : Equality Analysis

Completed by	**Reviewed by Marion Shipman,~**
Position	**Associate Director Quality and Governance**
Date	**1/5/2020**

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?			Consultation with Quality Assurance Board membership and Associate Director Data Security and Protection and DPO. Approval of the procedure. Implementation of good quality data and validation processes are used in and around the trust. A further step would be for more localised SOPs to be introduced.
If there is a greater effect on one group, is that consistent		X	

with the policy aims?			
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	
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 –seek advice from Human Resources.