East London NHS Foundation Trust

Clinical Data Quality Management Procedure

Version number :	3.0
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	27th October 2021
Name of originator/author:	Associate Director for Business Intelligence and Analytics / Information Governance Manager
Executive Director lead :	Chief Information Officer
Implementation Date :	September 2021
Last Review Date	August 2021
Next Review date:	August 2024

Services	Applicable
Trustwide	All Staff
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
2 Draft	October 2017	AD of informatics	Draft	Circulated for consultation prior to submission at November 2017 IGSG
3	August 2021	Associate Director for Business Intelligence and Analytics		

Contents

1. Introduction

1.1 High quality information underpins the delivery of effective patient care. The availability of complete, relevant, accurate and timely data means better patient care and patient safety. The management information produced from service user records is essential for the efficient running of the Trust and also supports robust clinical governance, healthcare planning, performance and accountability.

1.2 The importance of having data of the highest quality on which to base decisions, whether clinical, managerial, 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.

1.3 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.

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

1.5 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 is of the highest quality.
- Service planning – ensuring management can rely on the information to make informed and effective operational 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, IG Toolkit and NHSI Assessments.
- Good corporate governance – which, as above, has data quality as a pre-requisite to ensure effective strategic management.
- Legal compliance – ensuring that the Trust conforms to its legal obligations as laid down in relevant legislation, such as the 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

2.1 This procedure outlines the Trust's commitment to meeting high quality data standards. It sets out a clear framework for capturing and maintaining conformance with standards of data quality and is aimed at all individuals involved in the collection, recording, storage, processing and use of service user data.

3. Duties and Responsibilities

3.1 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.

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

3.3 The Senior Information Risk Owner (SIRO) acts as the advocate for information risk on the Board and oversees any risks related to clinical data.

3.4 The Chief Quality Officer 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.

3.5 The Information Governance Manager 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 IG toolkit submission.

3.6 The Chief Clinical Digital Officer is the link between clinical staff, informatics, and information governance. The Associate Medical Director for Clinical Information supports the improvement of the quality of the Trust's data by providing clinical insight to those managing the Trust's data in secondary use assurance.

3.7 The Associate Director of Performance provide guidance and support across a range of clinical data collection processes and advise on data quality improvements or changes necessary for reporting on the current and developing performance measures, such as CQUINs and KPIs. The individuals are responsible for actively monitoring, commentating on and supporting staff to improve performance trends.

3.8 The Clinical Service 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. Managers are responsible for managing the quality of data within their teams.

3.9 The Associate Director for Business Intelligence and Analytics is responsible for developing and validating reports based on commissioning and management requirements.

The Associate Director for Business Intelligence and Analytics ensures the Trust provides a focussed informatics service that supports the delivery of patient care, and produces and analyses a wide range of data and performance management information. This includes the production of high quality performance and contract compliance reports to the Trust Board, Service Delivery Board, Service and Clinical

Directors, Directorate Management Teams, Performance Managers and external commissioners and partners.

3.10 The Chief Quality Officer ensures that the Trust's informatics and storage of clinical information are operating safely, efficiently and effectively to discharge this procedure.

3.11 The Chief Digital Officer ensures that the Trust's digital systems, information technology, and information security systems are operating safely, efficiently and effectively to discharge this procedure.

3.12 Head of Contract Compliance 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 working closely with the Assistant Director of Informatics.

3.13 Clinical Staff have a responsibility to ensure the data they enter onto any system is of good quality and undertake regular data validation checks. Clinical staff are professionally accountable for the quality of information they submit, collect and use and may be held accountable for any data incorrectly recorded or not submitted.

3.14 All individuals who record information have a responsibility to ensure data is accurate, complete and captured in a timely manner. A fundamental principle of data quality is that data should be right first time which means responsibility is at the point at which it is collected and recorded. Individuals must ensure they read, understand and comply with this procedure, associated policies and any relevant local procedures and must advise their line manager of any factors affecting the production of complete, accurate and timely data. Day to day adherence to policies and procedures is a personal responsibility.

3.15 In addition, staff members must follow any local Standard Operating Procedures for the validation of data.

3.16 Data quality reports are tabled at the Information Governance Steering Group and Operations Meeting once per quarter.

3.17 All recipients of reports are required to routinely monitor data quality including local spot checks and request corrective action to be taken where necessary.

3.18 This procedure is applicable to all clinical 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.

3.19 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

4.1 Data quality is a measure of the difference between data collected against the experience of the subject (that is, the patient).

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

5 Data Quality Procedures

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

- Data Quality Standards
- Undertaking data validation
- Checking for and acting on missing or inconsistent data
- Managerial arrangements for quality and performance control
- Standard Operating Procedures
- Reports and dashboards

6 Data Quality Standards

6.1 Data standards ensure there is consistency in data collection by having agreed and implemented data definitions for key data items. These may be externally mandated or best practice.

Data must be:

- Accurate. All recorded data must be correct when the service user is registered and updated as appropriate thereafter to reflect both the service user's detail and the clinical pathway.

- Relevant. Data must not be superfluous and must meet current and future needs.

- Complete. All mandatory data items within a data set must be completed. Default codes will only be used where appropriate and not as a substitute for real data.

- Accessible. Data must be retrievable and must therefore be entered in the correct fields.

- Timely. All data must be recorded as soon after the event as possible according to the locally agreed timescales set out in Trust policies and procedures that will enable the data to be submitted in line with national deadlines.

- Valid. All data held on Trust electronic systems must be valid. Where codes are used these will comply with national standards or map to national values. Computer systems will wherever possible be programmed to accept only valid entries.

- Consistent. Data collection and recording must be consistent throughout the Trust to avoid ambiguity between different data sources and enable local and national comparisons to be made

6.2.1 Demographic Data. To ensure continuing accuracy of clinical records, the service user's full name, address and key contact details should be verified regularly at each contact. Electronic clinical systems and if appropriate paper records must be updated to reflect any changes.

6.2.2 The NHS number is the only unique way of identifying patients in the NHS system. It is imperative this is recorded correctly and used in all systems where patient information is present, including all correspondence. Detailed guidance is given in the Service User Identification Procedure and the Health Record Keeping Procedure.

7. Validation

7.1 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:

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

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

c. undertaking regular checks on service user data through rolling programmes of audit to check for completeness

d. validation of data entries

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

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

7.2 The following validation routines will be used:

- The Clinical Systems Manager will ensure that regular updates of appropriate national reference tables take place e.g. GPs and postcodes. If reference tables are incomplete the user must raise a request on the IT service desk portal https://eastlondon.service-now.com/sp

- The Associate Director for Business Intelligence and Analytics will ensure local tables are mapped to national codes in accordance with national data dictionary and dataset standards. Where local reference tables used for reporting are found to be incomplete or incorrect then the user should notify the Information team at elft-tr-Performance@nhs.net. Alternatively a request can be raised on the IT service desk portal https://eastlondon.service-now.com/sp However, inaccurate data must not be allowed to delay treatment of the patient.

- Accredited external sources of information such as the Personal Demographics Service (PDS) will be used to assist with the validation of records, particularly the NHS number.

- Regular validation processes will be undertaken on data to assess its completeness and accuracy e.g. checks for logical errors, duplicate records, incomplete or inconsistent data, missing NHS numbers.

- External sources of information such as reports from the Health & Social Care Information Centre, NHS Secondary user Services (SUS) will be used to ensure completeness and validity of records.

- Regular audits will be undertaken including CQUIN, Payment by Results, clinical coding and record keeping standards.

- Clinicians should be involved in validating data derived from the recording of clinical activity, including clinical coding purposes.

- Benchmarking of completeness of information on the Mental Health Service and Community Service and IAPT Datasets will be reported.

- Spot checks and comparisons between systems will be used to identify missing and inconsistent data.

- Up to date system operating or training manuals must exist for each system

- There must be written departmental procedures for the collection, validation and entry of data where these differ from standard operating procedures

7.3 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 cope 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.

7.4 Data Quality Assurance checks

These should be established by respective directors.

Clinical Data checks are run regularly by the Informatics department, and followed up by the Performance Teams via service leads and administrators, to improve data quality completeness and validity on reportable mandated fields (e.g. ethnicity, patient's postcode, registered GP) to ensure submissions to NHS Digital are as comprehensive and correct as possible.

The IG Toolkit requires an annual data quality assurance check to be undertaken and passed at a required level.

7.5 Management Arrangements for Quality Control

Team level day-to-day management of data quality lies with the respective team manager. SOPs may be employed to give guidance.

Directorate Management Teams will receive updates against key targets and standards from Quality and Performance Leads. Managers are responsible for reviewing and challenging any reported data that does not reflect members' understanding of practice/outcomes, as well as commissioning data investigations and monitoring action plans.

7.6 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.

7.7 Reports and dashboards

The Trust use reports from a number of systems, which include SQL Server, Reporting Services, Power BI and reporting from the clinical systems.

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

8. Training

8.1 All new contracted staff must attend an information governance induction training session, which includes instruction on data quality.

8.2 All new staff using clinical systems, or teams where a clinical system is introduced must attend training for that system and reporting services and may be further supported by workplace facilitation.

9. Monitoring

9.1 Performance in collecting and processing data will be routinely monitored and appropriate feedback provided to staff.

9.2 The Quality and Performance Managers also monitor clinical data and information from RiO EMIS, IAPTus, Nebula and other Electronic Clinical Record Systems RiO and more widely across the organisation and can be noted of any perceived data quality problems.

9.3 The Trust uses NHS Digital's Information Governance Toolkit as a way of providing a form of assurance of its management of information including assurance of data quality. Performance against the IG toolkit standards is considered by the Information Governance Steering Group. Assurance is provided to the Board via the Quality Committee.

9.4 Activity reports will routinely be sent to Performance and Operational Managers who must check and sign off reports within agreed time scales and take any necessary corrective action such as improving processes or staff training and development.

9.5 Directorate Management Teams should undertake local spot checks / audits to ensure accuracy of figures reported to the central Information team.

10. Related policies and procedures

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

- Information Governance and IMT Security Procedure
- Service User Identification Procedure

- Health Record Keeping Procedure
- NHS Number Procedure
- CPA Procedure
- Admission and Discharge Procedure
- Clinical Coding Procedure
- RiO crib sheets and procedures
- Reporting Services sheets and procedures
- Health Records Management Procedure
- Health Records Audit Procedure
- Code of Conduct on Confidentiality
- Data Protection Procedure
- Information Governance Policy
- Risk Management Strategy and Policy
- Records Retention Schedule
- Standard Operating Procedures may also exist locally

11. References

Data Protection Act: http://www.legislation.gov.uk/ukpga/1998/29/contents

NHS Information Governance Toolkit: https://nww.igt.hscic.gov.uk/