

# Data Quality Policy

*This is a controlled document. It should not be altered in any way without the express permission of the author or their representative.  
On receipt of a new version, please destroy all previous versions.*

## Document Information

<b>Date of Issue:</b>	Nov 2021	<b>Next Review Date:</b>	Dec 2024
<b>Version:</b>	V1.1	<b>Last Review Date:</b>	
<b>Author:</b>	Assistant Director of Information		
<b>Directorate:</b>	Information Team (Finance Directorate)		
<b>Approval Route:</b> Information Assurance Group			
<b>Approved By:</b> Information Assurance Group		<b>Date Approved:</b> 18/11/21	
<b>Document objectives:</b> The policy sets the duties with regards to data quality for all staff working for or on behalf of the Trust. It also confirms the ongoing approach to ensuring data quality standards are adhered to.			
<b>Intended Recipients:</b> All staff responsible for maintaining information and data within the Trust.			
<b>Links or overlaps with other Trust policies relating to:</b>			
TSDFT Information Governance Procedure			
TSDFT Information Governance Policy			
TSDFT Information Assurance Policy			

## Amendment Control/History

Issue	Status	Date	Reason for Change
V0.1	Draft	04/07/21	First Draft
V0.2	Draft	04/07/21	Draft Amendments – Submitted to IAG for review
V0.3	Draft	10/11/21	Draft Amendments – Submitted to IAG for approval
V1.0	Final Version	18/11/21	Approved by IAG
V1.1		10/11/23	Date extended to Dec 24

## Contents

1.	Introduction .....	4
2.	Purpose .....	4
3.	Scope .....	5
4.	Aim .....	5
5.	Roles & Responsibilities .....	5
6.	Governance .....	8
7.	Data Quality Standards .....	8
8.	Data Quality Procedures and Processes .....	10
9.	Monitoring Data Quality Issues .....	12
10.	Dissemination and Implementation of Policy .....	13

## 1. Introduction

Reliable information is a fundamental requirement for the Trust to conduct its business efficiently and effectively.

The benefits of using routine health data for planning, policy making and research are well established. Programmes are underway nationally and locally to use our data to build better and safer care through decision support systems. However, using data to augment direct care requires that data is high quality i.e. timely, complete and accurately coded.

There are many direct benefits for patients in improving data quality. This will ensure easier surveillance of patient safety, allows clinicians to use data confidently to drive local quality improvement initiatives and support new technology for direct care.

Poor data quality may lead to:

- Avoidable serious incidents occurring.
- Staff and service users being put at risk through invalid, or incorrect decisions being made about a service user's care.
- Lack of confidence in the validity of the recorded/reported information.
- Adverse results from the Care Quality Commission
- Poor management decisions relating to the Trust both internally and externally.
- Trust services being inadequately funded to provide responsive services to patient demands. This may happen where incomplete activity data does not provide complete evidence of demand and activity levels.
- Lack of credibility of the organisation and by implication of its profile and standing in the eyes of its peers, service users and carers and the public sector.

## 2. Purpose

The purpose of this policy is to set out roles and responsibilities and standards to ensure that the Trust operates with accurate and complete data and can meet its various legal and regulatory responsibilities. The policy is intended to;

- Confirm the Trust's commitment to a continual improvement in the quality of its data in order to support its business needs
- Confirm the Trust's ongoing approach to ensuring data quality standards are adhered to
- Inform staff working for, or on behalf of the Trust, of their duties with regards to data quality

The Data quality policy is an integral part of the Trust's approach to Information Governance and should be read in conjunction the [Information Governance Policies](#).

### 3. Scope

The policy will provide our staff working in every service area with clear guidelines as to their roles and responsibilities in respect of data quality. The scope and the principles set out in this policy are applicable to all information systems including both clinical and administrative

This policy applies to:

- All information that is held in either paper or electronic format.
- The development and implementation of any new information systems.
- All staff employed by or working on behalf of Torbay And South Devon NHS Foundation Trust who collect, use, input or report on information contained within the Trust information systems.

### 4. Aim

The aim is to provide and sustain a high level of data quality in order to provide meaningful information for corporate purposes, patient care and the delivery of external performance standards and targets. Ensuring information is robust is vital to meeting the Trust's business needs.

In order to achieve and maintain a high level of quality data it is important that the Trust puts in place processes for assessing, measuring, reporting, reacting to and controlling the risks associated with poor data quality.

This policy provides the framework for establishing, maintaining and improving the quality of data across TSDFT, and ensuring our data is regarded as fit for purpose in meeting the following standards;

- Valid
- Complete
- Consistent
- Accurate and up to date
- Relevant
- Available when required

### 5. Roles & Responsibilities

#### Chief Executive

The Chief Executive has overall responsibility for data quality.

#### Board of Directors

The Board of Directors have responsibility for setting the strategic context and for the formal review and endorsement of Information Governance policies and procedures including data quality.

#### Senior Information Risk Owner

The Director of Transformation and Partnerships is the Trust's [Senior Information Risk Officer](#) (SIRO) and is responsible for ensuring that the organisation's approach to information risk is effective. The Director of Transformation and Partnerships also has executive responsibility for the trust's Information Governance Function which sits in the Health Informatics Service Directorate. The Director of Transformation and Partnerships

chairs the Information Governance Steering Group whose remit includes oversight of the trust's Information Quality Assurance arrangements.

### **Information Strategy Executive Lead**

The Chief Finance Officer & Deputy CEO is the executive responsible for the overall strategic and operational direction of information management within the Trust.

### **Director of Health Informatics Service**

The Director of Health Informatics Service is responsible for trust's Information Governance function and the trust's quality assurance arrangements which includes maintaining policies and procedures for information quality assurance and the effective management of records in accordance with national standards

### **Information Manager**

The Information Manager is responsible for providing expert leadership in relation to data quality. The [Information Team](#) are responsible for identifying data quality concerns and finding solutions to enable data quality to be continuously monitored and improved by services/departments and Information Asset Owners.

### **Head of Data Engineering**

The Head of Data Engineering is responsible for processing and cleansing data in the Trusts data warehouse, and reporting data quality issues and exceptions. The Head of Data Engineering also chairs the trust's Information Assurance Group.

### **Information Governance Lead**

[Information Governance Lead](#) coordinates and manages the trusts Information Governance work programme..

### **Head of Service, Clinical Directors and Senior Managers**

Each Head of Service / Clinical Director is responsible for its data quality in their service/departments.

For all new staff joining the Trust, the importance of establishing the Trust's commitment to data quality should be addressed by the manager as part of induction as well as ensuring that all staff have read and understood the Data Quality Policy.

Managers should also ensure that all staff who need access to information systems have completed formal training at the commencement of their employment: this can be in classroom training sessions or via e-learning. Managers must also;

- Ensure that staff are aware of and comply with appropriate Trust policies and procedures and changes within policies are reflected in practice.
- Ensuring staff are aware of their responsibilities.
- Ensuring that support is provided to enable the timely, accurate and complete input of data onto the appropriate Trust information system.
- Ensuring that all staff are aware of their responsibilities with regard to checking and maintaining up to date data.
- Ensuring that any data quality issues identified are addressed quickly and reported to the Information Asset Owner and Information Asset Administrator.
- Ensuring that all working procedures are fully documented regularly updated and available to all staff.
- Monitoring staff knowledge and skills for using the information systems and identifying any training needs

- Monitoring compliance with this policy and appropriate use of information systems to ensure adherence with best practice requirement and data protection legislation.
- Ensuring that communication flows exist between the clinical and corporate services to facilitate the resolution of data quality issues.
- Ensuring that any data quality issues identified are addressed quickly and reported to the information asset owner.
- Ensuring that all job descriptions support the responsibilities within this policy and enforce the role's responsibility on ensuring accuracy and completeness of data.

### **All staff working within Torbay and South Devon NHS FT**

All staff who record patient information whether on paper or within electronic system have a responsibility to take care to ensure that the data is accurate, and complete as possible.

All staff including temporary or agency staff are responsible for:

- Compliance with relevant policies supporting documents. Failure to comply may result in disciplinary action being taken.
- Co-operating with the development and implementation of policies and as part of their normal duties and responsibilities.
- Ensuring the timely accurate and complete input of data onto the appropriate Trust information system or data recording sheets.
- Ensuring that they have the appropriate level of knowledge and skills for using the information systems.
- Where staff have responsibility for maintaining information but do not enter the data themselves they must provide input staff with the fully completed data sheets in a timely manner and ensure that the data entered is accurate and complete.
- Undertake regular validation checks of data collection and input to confirm that the data for which they have responsibility for is accurate, complete and up to date.
- Monitoring the data held for any data quality issues and reporting any concerns to the appropriate information asset owner or administrator.
- Identifying the need for a change in policy as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local or national directives and advising their line manager accordingly.
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training and awareness sessions as required or completing training materials when provided.

### **Information Asset Owner (IAO)**

The [Information Asset Owners](#) are accountable for;

- Maintaining data standards in accordance with national developments in relation to the system for which they are responsible.
- Ensuring that the system facilitates the collection of high quality data in accordance with national standards.
- Monitoring and disseminating changes implemented by information change notices.

- Establishing and disseminating monitoring reports from the system to appropriate staff and service detailing key data quality issues.
- Reporting any concerns to the appropriate service manager.
- Logging any information security issues / incidents relating to data quality with on the trust's Incident system (Datix).

## 6. Governance

### Information Assurance Group

The [Information Assurance Group](#) is responsible for;

- Overseeing the development and oversight of the implementation of the Trusts data quality improvement workplan
- Ensuring completion of national requirements are met and reviewed annually. (Including national requirements, such as the data quality maturity index)
- Escalating data quality issues to the appropriate committee
- Ensuring incidents around data quality and accuracy are investigated appropriately to enable to Trust to identify root causes and escalate risks.
- Agreeing and reviewing performance against external and internal data quality KPIs and ensuring that appropriate improvement actions are carried out as appropriate.

The Information Assurance Group is accountable to IM&T Group

### The Information Governance Steering Group

The [Information Governance Steering Group](#) is responsible for;

- Directing and performance managing the development and implementation of data quality assurance policies and procedures as part of the wider information governance agenda.
- Monitoring the Trust's information handling activities to ensure compliance with the law and NHS policy and guidance
- Escalating data quality risk to the appropriate committee

## 7. Data Quality Standards

### Validity

All data items held on all Trust computer systems must be valid. Clinical systems should be configured in line with relevant Information Standards and NHS Data Models. Where possible information systems will be configured to provide appropriate levels of validation at the point of entry in order to quality assure data critical to the provision of high-quality care, clinical and operational decision making and performance monitoring.

Data must be clinically valid, for example information such as the appropriate outcome measures, clusters or diagnoses or demographics such as address or date of birth must accurately reflect the patient's situation. The correct recording process and structures must be used to record the data and data must be entered into the Trust systems in accordance with the standard operating procedures and guidance.

### Completeness

All staff entering data into any of the Trust systems are required to complete all of the mandatory data items.



Internal systems should provide reports that service managers and operational staff will use to maintain data completeness. All mandatory data items within a data set should be completed. Use of “unknown” or “not stated” codes will only be used as a last resort, and not as a substitute for real data. If it is necessary to bypass a data item (for example, in order to admit a patient into hospital), the missing data should be added as soon as practical

Clinical teams are expected to identify missing items and check with the patient to complete the data.

### **Consistency**

Data items should be internally consistent. Patients with multiple episodes must have consistent dates. Diagnoses and treatments must be consistent for ages and sex and must be coded in line with clinical coding guidance and in line with the trust clinical coding policy.

### **Coverage**

All relevant data must be recorded for all Trust systems. For clinical systems all work relating to patient care provided by the Trust must be recorded. This includes Inpatient admissions, outpatient attendances, day care and community contacts.

Correct procedures are essential and should be followed by all staff recording any of this information to ensure complete data capture. Data Quality reports and spot checks and analysis must be used to identify missing data.

### **Accuracy**

Data must be checked for accuracy by both clinical and non-clinical staff to ensure that the correct information is recorded on Trust systems.

For clinical systems, data recorded in notes and on computer systems must accurately reflect what activity happened to a patient and when.

Each service/department is responsible for ensuring that every opportunity is taken to check patient’s demographic details with the patient themselves. Inaccurate demographics may result in records being mislaid, or incorrect identification of patient. Checks on patient data should be done at every appointment or review to ensure that the most up to date information is held by the Trust.

The protected characteristics also known as ‘special category data’ (including race, religion and belief, sexual orientation and disabilities) of service users must be collected and regularly monitored for accuracy in the same way.

All reference tables, such as GPs and postcodes, must be regularly updated. This will usually be within a month of publication unless there are serious doubts about the quality of the data supplied.

### **Timeliness**

Data must be entered onto Trust systems in a timely manner to ensure that up to date information is recorded on Trust systems.

Recording of timely data on inpatient stays, day care, community contacts, outpatient appointments etc. is vital to the care of the people using our services. Any updates to a patient record should be recorded onto the clinical system as soon as possible and no later than 1 working days.

Trust Systems must be kept up to date. This is essential to ensure that they accurately reflect the activity undertaken by the Trust and to accurately reflect changes to national standards and data definitions. Mechanisms will be established to ensure that updates are disseminated efficiently and effectively.

## **8. Data Quality Procedures and Processes**

### **Key Data Quality Procedures and Processes**

Careful monitoring and error correction can support good quality data, but it is more effective and efficient for data to be entered correctly first time. In order to achieve this, good procedures must exist so that staff can be trained and supported in their work.

Standard operating procedures must be put in place for each information asset to facilitate the capture of data. These standard operating procedures must ensure adoption of information standards published by NHS Digital on their [Information Standards website](#).

Procedures are detailed descriptions of the processes by which policies are carried out and should contain details of:

- The person in overall control of the policy or process
- Other persons involved
- Any definitions appropriate to the document

As a minimum for clinical systems the following procedures will be documented:

- Registering a referral
- For all patients recording activity, contacts, appointments, failures to attend and cancellations, outcomes from attendance
- Managing waiting lists
- Recording assessments, outcome measures and clusters
- Recording details of clinical activity and clinical coding
- Recording discharge arrangements
- Managing duplicate and confused records

The data quality elements of any procedure must be defined in a way that is clear and unambiguous to any person expected to carry out the tasks. They should reflect national and local standards

Procedures should be reviewed at least once a year to take account of any changes in national standards and definitions. Tight version control is essential so that staff in all parts of the Trust are using the same procedures which reflect current data definitions. Procedures should be published on the Trust intranet.

The accurate recording of data items must not be allowed to delay urgent treatment of a patient. But also need to ensure that the data is accurate in order to deliver the correct and appropriate treatment.

### **System Operating Procedures**

It is the responsibility of each manager to ensure that all relevant staff who will use information systems completes formal training.

The environment in which users work is important in terms of data quality. Supervision

of staff using computer systems must allow working practices that enhance quality work, such as:

- Adequate breaks
- Refresher training
- Reasonable workload
- Access to training manuals – hard copy or on the Intranet
- Work stations which comply with health and safety legislation

## **Training**

All staff should receive appropriate data quality training and awareness sessions to ensure that they understand the importance of collecting and recording complete and accurate information to minimise the risks to the service user and to the organisation itself. The use of examples and scenarios may be particularly useful to ensure that a basic level of competence has been achieved before access to the systems is allowed.

Some staff may be required to have higher levels of awareness relating to data quality to carry out their duties. Where this is the case appropriate additional training should be provided according to staff job roles, level of access to person identifiable information and responsibilities for processing/managing records. The training programme must cover all aspects of data quality including:

- The definition of individual data items - so that staff know what they are recording
- The eventual use of data – so staff understand what the data they are recording will eventually be used for (and therefore why it is important to record accurately)
- The function of data items – so staff know the purpose of recording
- How to validate data with the service user or against the health care record – so checks are carried out to confirm the accuracy of data

## **Audit Trails**

It is vitally important that activity can be traced back to a user, so that any erroneous, inaccurate or incomplete data can be identified and rectified by the original user.

All clinical systems must have an audit trail that is turned on and used. Audit trails are used to identify errors. No password or account sharing should take place on any Trust systems. Account sharing lets potentially unauthorised and untrained individuals have access to service user information.

Anyone who has concerns about any data recorded should in the first instance refer this to their line manager. Data quality incidents should be raised on the Trust's incident system (Datix)

## **Risk Management**

Information collected on the Trust's information systems is used to inform clinical care, manage resources, record financial flows and to improve services within the Trust. If data is not collected efficiently and effectively a number of risks can occur.

- Incomplete or inaccurate demographic details can impact on patient care.
- The inconsistent collation of key data items may result in unsuccessful and ill informed decisions for service improvement
- The inaccurate recording of contact information can impact on resources.
- Poor data quality presents a risk to planning and performance management
- Failure to record key data items may result in a lack of payment for Trust services by commissioners

Regular monitoring of data quality risks should be in place. Any identified data quality risks should be should be raised on the Trust's incident system (Datix).

### **Business Continuity**

When this process is invoked, care should be taken to ensure the accuracy of data entry from handwritten paper records. Regular checks should be carried out to give assurance of data quality in these circumstances.

## **9. Monitoring Data Quality Issues**

### **Measurement of Good Data Quality**

Data quality will be subject to control processes within the Trust and will also be subject to external scrutiny. The Trust compliance with national data quality standards will be measured externally via;

- The Data Quality Maturity Index (DQMI) published by NHS Digital
- The SUS DQ Dashboards published monthly by NHS Digital for the three Commissioning Datasets (CDS); Admitted Patient Care (APC), Outpatients (OP) and Emergency Care (ECDS)
- The Hospital Episode Statistics (HES) Data Quality Notes published regularly by NHS Digital contains additional data quality information following additional processing on the three Commissioning Datasets (CDS) submitted through the Secondary Uses Service (SUS)
- National dataset specific data quality reports published at point of submission by NHS Digital through the Bureau Services Portal for collections
- Dataset specific data quality reports (on both local and national datasets) processed by Data Services for Commissioners (DSfC) and issued via Commissioning Support Units (CSUs) and supplied direct or via commissioners
- Third party services from organisations who use open data published by NHS Digital and other health care bodies to provide benchmarking and clinical coding assurance tools

### **Internally**

Data quality monitoring reports must be established for internal systems to reports on data validity for clinical data items such as inactive referrals, ethnic group, patient outcomes and NHS numbers. These reports should be used to improve processes, identify training needs and documentation.

Audits of Data Quality should be conducted and the audit results circulated to the Service Managers and Information Asset Owners.

### **Identifying and correcting errors**

Errors must be corrected as soon as possible after identification. This will be at the latest within one week of identification of error. In most circumstances this will be the responsibility of the person who entered the incorrect information; where this is not possible, someone within that person's team/service must take responsibility for doing it.

All information from clinical systems reported to the Board and external partners must be first circulated to Operations for approval. Service Managers are responsible for reviewing these reports, identifying where the errors occurred and advising teams to correct data on systems if required.

## **10. Dissemination and Implementation of Policy**

The policy is available on the ICON [Intranet](#). Implementation of the policy will be the responsibility of all staff, with particular responsibility with team managers as documented in relevant sections. All new staff are required to attend relevant training courses before using Trust information systems.