Shropshire Community Health NHS
NHS Trust

Information Quality Assurance Policy

Controlled document

This document is uncontrolled when downloaded or printed

Author(s)
Owner(s)
	Author: Steve Price, Information Programme Manager
	Owner: Steve Price, Information Programme Manager

Version No.	Version 1.3
Approval Date	7th April 2022
Review Date	7th April 2025

Shropshire Community Health NHS Trust
Policies, Procedures, Guidelines and Protocols

Document Details	
Title	**Information Quality Assurance Policy**
Trust Ref No	1340-73640
Local Ref (optional)	N/A
Main points the document covers	This policy details the arrangements to ensure the availability of complete, accurate and timely data in supporting patient care, clinical governance and management functions
Who is the document aimed at?	All staff, especially those who provide and manage data
Owner	Steve Price (Information Programme Manager)
Approval process	
Approved by (Committee/Director)	Data Security and Protection Assurance Group (DSPAG)
Approval Date	7th April 2022
Lead Director	Director of Finance
Category	General
Sub Category	Information Governance
Review date	7th April 2025
Distribution	
Who the policy will be distributed to	All staff
Method	Publication on the Trust website
Document Links	
Required by CQC	Yes
Required by NHLSA	No
Other	Data Security and Protection Toolkit

Amendments History		
No	Date	Amendment
1	February 2013	Minor amendments throughout document and update to Section 9 – Measuring Good Quality Data
2	November 2014	1. Added in an additional section **Managing data quality** (section 5) 2. Updated the communication section. 3. Other minor amendments throughout document. 4. Updated supporting guidance links.
3	November 2015	1. Sections 7.4 and 7.5 – replaced reference to Information Governance Committee with IM&T Strategy group. 2. Updated section 9.3 with the inclusion of reference to EPR 3. Updated codes of practice and standards in section 6.2 4. Other minor amendments throughout document.

4	November 2018	1. Review and update of terminology, references and standards across all sections. 2. Update of Scope to include Information Asset Owners 3. Updated Procedures 4. Managing Data Quality section updated to specify responsibility for documenting procedures 5. Update to Roles and Responsibilities
5	October 2019	1. Update to section 7.12 to include reporting data quality incidents where applicable
6.	January 2022	1. Review of policy against DSPT Assertion 1.1.7 – conducted by Templar Consultancy.
7	February 2022	1. Review of Policy against DSPT Assertion 1.1.7 2. Updates to reflect changes to naming, reporting governance, dates relating to acts/codes of practice and national standards 3. Update to Information Asset Owner and Admin definition / responsibilities 4. Addition of Appendix 1 – Data Quality Procedure Template 5. Addition of system front end DQ validation 6. Update to improvement plans being reviewed at DSP Assurance Group instead of approved 7. Updated Communications

Contents

1. Introduction 5
2. Scope of the Policy 6
3. Purpose 6
4. Procedures 7
5. Managing Data Quality 8
6 Legal Requirements 9
7 Roles and Responsibility for Data Quality 9
8 Supporting Structures 11
9 Data Quality Standards 12
10 Measurement of Good Data Quality 14
11 Communication 14
12 Guidance 15
Appendix 1 16

1. Introduction

1.1 Patients, staff and stakeholders expect their data to be up to date and accurate. Shropshire Community Health NHS Trust (hereafter referred to as the Trust) recognises the importance of reliable information as a fundamental requirement for the speedy and effective treatment of patients, management of staff and stakeholder contracts. Data quality is crucial, and the availability of complete, accurate and timely data is important in supporting patient care, clinical governance and management and service agreements for healthcare planning and accountability.

1.2 This policy sets out a framework which is designed to help the Trust ensure a high standard of data quality across all the Trust's information. The overall aim is to ensure that the Trust's data is fit for purpose and support the delivery of high-quality care and decision making.

1.3 The importance of good data quality in the NHS has never been more important. Poor data quality can have serious consequences. It can:

- Put vulnerable people at risk – poor or missing data can lead to mistaken identity or missed alarms about an individual or quality of care.
- Weaken frontline services – good data empowers professionals working at the front line, but poor data can lead to poor care and wasting clinical time on validation.
- Lead to financial loss and poor value for money – missing data can lead to lost income for the Trust and compliance breaches. It can also mean that inefficient processes are not identified.
- Undermine accountability and damage trust – without good data, informed decisions cannot be made, and misleading data can lead to reputational damage.

1.4 Good quality data is accurate, valid, reliable, timely, relevant and complete:

- **Accuracy** – data should be sufficiently accurate for the intended purposes.
- **Validity** – data should be recorded and used in compliance with relevant standards.
- **Reliability** – data should reflect stable and consistent data collection processes across collection points and over time.
- **Timeliness** – data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period.
- **Relevance** – data captured should be relevant to the purposes for which it is used.
- **Completeness** – all of the relevant data should be captured.

1.5 Good data quality is not an optional extra. It is a fundamental basis for the business of the Trust. As such it should always be considered at the centre of any future developments and kept under review.

1.6 Ever increasing use of computerised systems provides greater opportunities to store and access many types of data but also gives rise to new risks, which this policy seeks to address.

1.7 Some of the patient data, e.g. for Community Hospital Inpatients and Outpatient Clinics, is sent outside the Trust to national databases via the Secondary Uses Service (SUS), so data has a wider audience than just the originating organisation. Consistency and compliance with national standards are, therefore, essential as the Trust is measured and judged on the data which it produces.

1.8 Health Service indicators (Data Security Protection Toolkit, DSPT) also depend on good quality data. In addition, the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 requires amongst other things, that information held is accurate and up to date.

1.9 This policy raises the profile of data quality and defines the appropriate data quality responsibilities for everyone in the Trust.

2. Scope of the Policy

2.1 All Information Systems within the Trust (both electronic and paper based) fall within the scope of this policy.

2.2 The Trust Information Systems include Electronic Patient Record Systems, Patient Information Systems, Finance, Risk, Human Resources and Payroll databases.

2.3 All Information Systems must be registered on the Trust’s Information Asset Register and assigned an Information Asset Owner

3. Purpose

3.1 The purpose of this policy is to:

- Define the levels of responsibility throughout the Trust for data quality
- Highlight the legal requirements concerning data quality
- Ensure the recording and presentation of data to the highest possible quality giving all users of the information confidence in its accuracy

4. Procedures

4.1 Data quality will be measured and reported using a wide spectrum of measures and indicators, which will ensure that data is meaningful and fit for purpose. Measures and indicators used to monitor data quality may include:

- Completeness checks
- Accuracy checks
- Validity checks
- Timeliness checks

4.2 Each Service Manager will measure and improve the completeness and validity of key data items on their systems.

4.3 Key data items, for clinical systems, which must be collected and recorded, include:

- First name
- Last name
- Date of Birth
- NHS Number
- Address, including Post Code
- Contact telephone number
- Gender
- Ethnicity
- GP Practice
- Spoken Language

4.4 The NHS Number is used as the common identifier for patients across different NHS organisations and is a key component of the NHS Care Record Service (CRS). In accordance with the NHS Number national standard the Trust will aim to achieve 100% usage of the NHS Number on all electronic and manual clinical systems. The NHS Number must be used in all internal and external service user/patient related Trust correspondence.

4.5 The Trust will conduct an annual accuracy audit of Trust Information Systems that contain Personal Confidential Data (PCD) in line with information governance guidance. This audit will be reported to the DSP Assurance Group via the Data Quality Sub-Group.

4.6 Completed audits will be held in the Trust’s document management system, SharePoint.

4.7 Procedures and policies must be in place to ensure that a high standard of data quality is maintained for all data captured and recorded.

4.8 The Trust Information Systems and any associated procedures will be updated in line with national requirements for example, as currently notified by Information Standards Notice (ISN)

4.9 The Trust policies and procedures will be updated in line with any national changes and following an annual review of the Information Governance requirements.

5. Managing Data Quality

5.1 The Trust's Information Asset Owners, in conjunction with Service Managers, will be responsible for establishing a documented data quality procedure which describes how data quality is maintained, monitored and improved.

5.2 The length and level of detail in each procedure will vary depending on the nature of the information system and how the data is used. A simple template is included in appendix 1. As a minimum each data quality procedure should include sections on:

- **Data standards** – what standards are expected on areas such as timeliness of data capture (how long after the event is acceptable), completeness of data (what key data items must be captured)

- **Data quality assurance** – how is compliance with data quality standards monitored, are there any data quality KPIs and where are these reported.

- **Data quality improvement:**

  - How completeness and validity issues that are identified are investigated and rectified.
  - Training and guidance - how system users are trained to ensure good data quality and what guidance is available to them on data quality standards and procedures to ensure good data quality.
  - The steps that are taken to target users who are responsible for repeated data errors. E.g. after three errors in a six month period staff are required to be retrained in the use of the information system.

5.3 Some systems may also require sections covering.

- **External data quality reports and benchmarking** – these will detail the external data quality reports available (e.g. from NHS Digital), how these are used and how the data quality is benchmarked against other organisations.

- **Completeness and validity checks** – detailing any nationally and locally mandated checks on the completeness and validity of data.

- **Validation and audit** – how the accuracy of the data is validated, and the auditing procedures in place.

- **Maintaining data quality** – how data quality is to be maintained when there is a change to clinical services or the management structure of the Trust.

- **Links to other systems** – are there any other systems which depend on this system for their data – if yes then a documented data quality procedure needs to define how the quality of the information passed between systems is maintained.

6 Legal Requirements

6.1 Legislation has a significant effect on Information Governance in NHS organisations. The Trust must ensure that all policies and procedures are fully compliant with legislation and NHS guidance on the management of information.

6.2 The following acts, codes of practice and standards place a statutory duty on the Trust to ensure the completeness and accuracy of data. These include but are not limited to:

- Data Protection Act 2018.
- UK General Data Protection Regulation (UK GDPR)
- Data Security and Protection Toolkit
- Codes of practice for handling information in health and care
- Freedom of Information Act 2000.
- Records Management Code of Practice for Health and Social Care 2021

7 Roles and Responsibility for Data Quality

7.1 The **Chief Executive** has the ultimate responsibility for data quality.

7.2 The **Trust Board** has overall responsibility for monitoring data quality. They monitor data quality via key performance indicators (KPIs) included in the performance report.

7.3 Through the Information Governance Framework, the **DSP Assurance Group** will report on the progress against the action and recovery plans relating to data quality issues. The Data Quality Sub-Group is a specific working sub-groups, for data quality, to deliver particular specialised parts of the data quality agenda under the remit of the DSP Assurance Group and that group will agree their terms of reference

7.4 The **Information Programme Manager** is responsible for overseeing the management of data quality, in conjunction with other managers e.g. Records Manager; by ensuring compliance with NHS standards.

7.5 The **Information Asset Owners** in conjunction with Information Asset Administrators and Service Managers, are responsible for ensuring that data quality checks are conducted in accordance with this policy and other national guidance.

7.6 The **Information Governance Manager** has an interest in data quality in ensuring compliance with the seven principles of the UK GDPR and Data Protection Act 2018.

7.7 The **Freedom of Information lead** has a responsibility to ensure that the Trust provides data quality in order to comply with the FOI Act 2000.

7.8 **Service & other Managers** are responsible for:

- Ensuring that the information recorded by their staff meets the data quality principles outlined in section 1.
- Delivery of periodic audits of the accuracy of data recorded.
- Monitoring the data quality in relation to system developed reports produced by their staff.
- Implementing data quality management processes such as regular Data Quality Audits, retraining programmes.

7.9 There will be identified individuals within the **Informatics Department** with the responsibility for producing data quality reports and liaising with service managers on data quality issues.

7.10 **All staff** who record information, whether on paper or by electronic means have a responsibility to take care to ensure that the data is accurate and as complete as possible. Individual staff members are responsible for the data they enter onto any system.

7.11 All members of staff are responsible for ensuring any identified errors are reported to the appropriate manager using the data quality procedures in place and reported via the Trust’s incident management process where applicable.

7.12 All data must be entered carefully and checked at point of entering. Following defined procedures, best practice and taking care when entering data will significantly reduce mistakes and other simple errors.

8 Supporting Structures

8.1 The importance of establishing the Trust's commitment to data quality should be addressed at the commencement of employment by the appointing officer.

8.2 The responsibility for user training and system access control will depend on the system being used. For example, if it is a service specific clinical database then responsibility falls to that service.

8.3 In accordance with the Trust's Learning, Development and Study Leave Policy and the Data Protection Policy all staff must complete appropriate training e.g. role specific.

8.4 Users should only be allowed access to a system once adequate training has been completed.

8.5 All staff at the commencement of employment must sign a confidentiality agreement and be made aware of Trust policies and procedures relating to confidentiality and security.

8.6 Further information on data security can be found in the Trust's **Information Security Policy.**

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

8.8 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
- Workstations which comply with health and safety legislation

8.9 All major data entry systems must have an audit trail facility which are turned on and used.

8.10 Any training issues identified in audit must be addressed promptly.

8.11 All users should be made aware of the Trust's Whistle Blowing Policy. This allows individuals who may have concerns about data and are experiencing difficulties in resolving them in the normal way, the opportunity to relay them to an appropriate senior member of staff.

9 Data Quality Standards

9.1 **NHS Number** (*Direct Patient care) – The NHS Number is the primary patient identifier in the NHS.

**Direct patient care – activity carried out which is directly linked to the patient's treatment (e.g. Appointments, procedures, medical records)*

9.2 The NHS Number should be used in all correspondence as the key identifier to reference patients who have their data stored electronically or on paper records.

9.3 The NHS Number should be quoted in all correspondence about a particular named patient. The only exceptions are for patients who do not have an NHS Number (e.g. patients from Scotland or Overseas) when a suitable alternative means of identification shall be used (e.g. Community Health Index Number for Scottish patients.)

9.4 NHS Number (**purposes other than direct care of patients) – It is the NHS policy that patient level data should not contain identifiers, including the NHS Number when it is used for purposes other than direct care of patients.

** Purposes other than direct care of patients – activity carried out which does not have a direct impact on the patient treatment. (e.g. raising of invoices, aggregated activity counts, commissioning of services)

9.5 The Trust has a function in place for data/ information that is required for secondary use and has been anonymised or in which identifiers have been replaced with pseudonyms. Refer to the Trust's Information Governance Policy for further guidance around Pseudonymisation and anonymised records.

9.6 **Validity** - all data items held on Trust computer systems must be valid. Where codes are used, these will need to comply with national standards or will map to national values e.g. NHS Data Dictionary. Wherever possible, computer systems will be programmed to only accept valid entries.

9.7 **Completeness** – all mandatory data items within a data set should be completed. Use of "unknown" codes must 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.

9.8 **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.

9.9 **Coverage** – data will reflect all the work done by the Trust. Admitted patient care (inpatients), outpatient attendances, and community contacts should all be recorded. Correct procedures are essential to ensure complete data capture. Data Quality reports and spot checks should be used to identify any missing data.

9.10 **Accuracy** – data recorded in notes and on computer systems must accurately reflect what happened to a patient**.**

9.11 **Timeliness** – recording of timely data is beneficial to the treatment of the patient. All data must be recorded in advance of national contractual and local reporting deadlines. The accurate recording of data items must, however, not be allowed to delay urgent treatment of patients.

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

9.13 Where available, national data standard definitions should be used within systems e.g. NHS Data Dictionary

9.14 Every opportunity should be taken to check patient's demographic details with the patient themselves. It is important that the patient provides their details to staff, rather than staff telling the patient their details. Inaccurate demographics may result in records being mislaid, or incorrect identification of patient.

9.15 Recording of diagnosis and treatments makes that information available to all staff with a legitimate relationship treating the patient, even if they do not have access to the paper notes.

9.16 **Documented Procedures** – 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. Details of these procedures, training and processes must be available within each service.

9.17 **Identifying and correcting errors** – errors should be identified as close to point of entry as possible. This will be done by:

- Data quality checks that may exist in the front end of a system and which conform to national standards where they exist. Data entry screens should be designed to be as efficient as possible to aid the data entry process, and field validation enforced if possible
- A program of weekly/monthly error reports, produced by the Informatics department, forwarded to the appropriate Service representative. This will be documented in the procedures outlined in section 5
- Investigation of external Data Quality reports

- Secondary Uses Service
- Additional checks requested by services

10 Measurement of Good Data Quality

10.1 The Trust will ensure that it can demonstrate to itself and external bodies that it is maintaining accurate information about its services and service users.

10.2 Data quality will be subject to control processes within the Trust and will also be subject to external scrutiny.

10.3 The Trust will aim to be significantly above average in all indicators and will strive for 100% accuracy.

10.4 The Trust will act on all enquiries and complaints from Commissioners or Patients.

10.5 Internally – the Data Quality Sub-Group will report to the Trust's DSP Assurance Group at their regular meetings. Updates will be provided to the group on the progress from the Trusts data quality audits and data items, which have been identified as causing concern (e.g. NHS Numbers, ethnic group, coding, completeness), improvement action plans for areas identified as causing concern will also be reviewed.

10.6 Internal monitoring reports will be used to inform management, to improve processes, identify training needs and further documentation.

10.7 Externally – the following mechanisms are used by the Trust as external measurements of data quality

- Data Quality reports
- Data Quality Maturity Index (DQMI)
- HES/SUS Data Quality Indicators
- Community Service Dataset (CSDS)
- Queries from Commissioners
- Queries from patients
- Audits

11 Communication

11.1 This policy will be disseminated to staff by the following methods:

- Data Security and Protection Assurance Group
- Digital Programme Group

- Trust Board
- Trust Communications
- Trust Website

The Trust will raise awareness on all topics covered in this policy through the Trust's Induction and mandatory training programmes.

Managers should continue to raise awareness through the appraisal process and service/departmental Team Meetings.

11.2 From time to time new data quality standards appear which may have an impact on the quality of data recorded (e.g. an optional data item becomes a mandatory one).

The Trust will disseminate such standards through the appropriate members of the Data Quality Sub-Group

12 Guidance

12.1 The following guidance can be read as a support to this Policy:
Information Standards and Collections (Including Extractions) - National Governance:
https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions
NHS Codes of Practice and legal obligations: https://digital.nhs.uk/

12.2 Shropshire Community Health NHS Trust related policies and guidance include but are not limited to:

- Information Security Policy
- Information Risk Policy
- Registration Authority Policy
- Data Protection Policy
- Records Management Policy
- Clinical Record Keeping Policy
- N365 Policy

Policies can be found in Policies Library on Public Website and Staff Zone

Appendix 1

Standard Data Quality Procedure Template

Asset

- Description/Name of system used

Service

- Name and description of the service including specific teams covered

Data Standards

- Timeliness of data capture (how long after the event does the service have to enter data)

- Completeness of data (List the data items that are important and must be captured)
    - ***For example***
    - Referrals
        - Received Date
        - Service
        - Referral Reason
    - Appointments
        - Date
        - Clinic
        - Outcome

Data Quality Assurance

- How are the standards going to be monitored? i.e. aggregated report from Data Warehouse/Information, HR, Finance

- Do you receive reporting that details compliance i.e. that NHS Number capture is at 95% or that the data is entered within 2 days for 98% of the time? If so, outline here or discuss with team that provides reporting

- Do you have Key Performance Indicators (KPI) showing performance of data quality items?

- Whose role is it to monitor data quality for the service and take action where needed?

Data Quality Improvement

- Whose role is it to investigates issues?

- How are issues investigated and rectified?

- How are your users trained to ensure good data quality?

- Are users with a history of repeated data errors supported with further training?

External data quality reports and benchmarking

- Detail of external data quality reports that are available
- How are external data quality reports and benchmarking used?
- How these are benchmarked against other organisations

Completeness and validity checks

- Detail any nationally and locally mandated checks on the completeness and validity of data.

Validation and audit

- How the accuracy of the data is validated, and the auditing procedures in place.

Maintaining data quality

- How data quality is to be maintained when there is a change to clinical services or the management structure of the Trust.

Links to other systems

- Are there any other systems which depend on this system for their data – if yes then a documented data quality procedure needs to define how the quality of the information passed between systems is maintained.