NHS
Yorkshire
Ambulance Service
NHS Trust

Data Quality Policy

Document Author: Head of Business Intelligence

Date Approved: February 2026

Document Reference	PO – Data Quality Policy – February 2027
Version	V: 9.0
Responsible Director (title)	Chief Information Officer
Document Author (title)	Head of Business Intelligence
Approved By	Information Governance Working Group
Date Approved	February 2026
Review Date	February 2027
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
2.0	March 2007	David Johnson Assistant Director of IM&T	A	
3.0	March 2014	Stephen Graham Business Intelligence Manager	A	Approved by Senior Management Group subject to minor amendments to sections 3.2.4 and 6.2.
4.0	March 2016	Nigel Batey, Business Intelligence Manager	D	Full Review
5.0	March 2020	Nigel Batey, Head of Business Intelligence	A	Approved by TMG
6.0	March 2021	Risk Team	A	Approved by TMG
7.0	July 2022	Risk Team	A	Approved at TMG
7.1	November 2023	Alex Bell	D	Review Policy – no changes required
8.0	February 2024	Risk Team	A	Approved in February 2024 Information Governance Working Group
8.1	January 2026	Nigel Batey	D	Policy reviewed – no changes required
9.0	February 2026	Risk Team	A	Policy approved within February 2026 Information Governance Working Group
A = Approved D = Draft				
Document Author: Nigel Batey, Head of Business Intelligence				
Associated Documentation: • Information Governance Framework • Information Sharing Policy • Records Management Policy • Data Protection Policy • Email and Communications Policy				

Staff Summary

All Staff have a responsibility for data quality and must know and follow Trust procedures relating to data quality management and have attended relevant training or awareness sessions. All staff to be aware of their GDPR responsibilities.
Information Asset Owners (IAOs) should be identified for each electronic or manual system. The IAO is responsible for the quality of data on their system and compliance with relevant legislation and NHS standards.
All Staff must follow Trust procedures for recording data in an accurate and timely manner via paper based or electronic means
All new staff that are to use paper based and electronic information systems will receive appropriate training in the use of the respective systems from appropriate trainers, following approved training plans and learner outcomes. This will include Information Governance induction and mandatory training, as included in the Trust's Training Needs Assessment in the Statutory and Mandatory Training Policy.

1.0 Introduction

1.1 Yorkshire Ambulance Service NHS Trust ('the Trust') places strong emphasis on the availability and integrity of information to assist in the effective delivery of care to service users, service management, performance management, corporate governance, internal and external accountability and communication. The Trust is also committed to supporting its local health community through the provision of information and analysis to external stakeholder groups and partners.

1.2 The Trust recognises the importance of reliable information to the safe delivery of patient care. Data quality is crucial, and the availability of complete, accurate and timely data is important in supporting patient care, clinical governance, corporate governance, management and service level agreements for healthcare planning and accountability.

1.3 Data Quality, or Information Quality Assurance as it is alternatively termed, is an integral part of Information Governance and is recognised by the Department of Health as a Key Performance Indicator for healthcare organisations. The Trust must demonstrate effective arrangements to ensure that the use of information complies with legal, regulatory and best practice requirements.

1.4 A Data Quality Framework will be available for staff with tools to use to embed the Data Quality Principles set out in this document.

2.0 Purpose/Scope

2.1 The purpose of the policy is to:

- Establish the Trust's commitment to data quality and its approach to ensuring data quality standards are adhered to.
- Inform all staff working for, or on behalf of the Trust, of their roles and responsibilities with regards to data quality.
- Maintain and increase high levels of data quality within the Trust.

2.2 The principles contained within this policy will provide a framework for all staff which will facilitate the development of departmental data quality procedures to ensure that data collected and recorded is accurate, fit for purpose and available when required.

2.3 This policy should be read in conjunction with other related policies and forms an integral part of the Trust's approach to the governance of data.

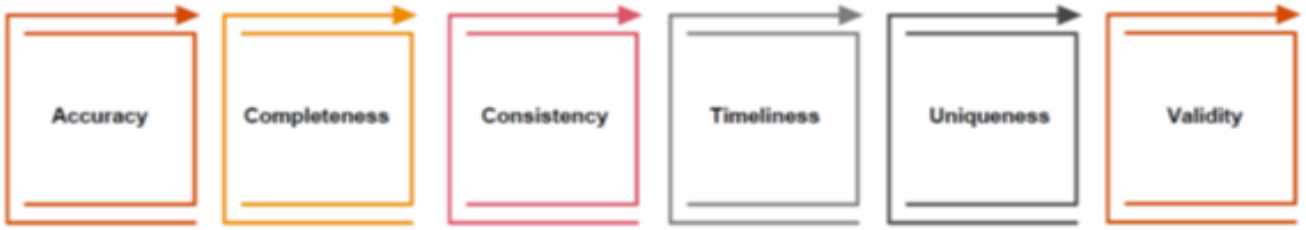
2.4 **Why is Data Quality Important?**

2.4.1 The Trust makes extensive use of data and information to make strategic and operational decisions to assist the delivery of quality patient care, service management, performance management and corporate governance. The Trust relies on the availability and integrity of this information to support these decisions.

2.4.2 Data and information from the Trust is used externally by various organisations to support the management, governance and service level agreements for healthcare planning and accountability. The Trust must ensure the information supplied is timely, accurate and reliable to support these decisions and protect the Trust's reputation.

2.4.3 Data quality is an integral part of Information Governance and is recognised by the Department of Health and Social Care as a Key Performance Indicator for healthcare organisations. The Trust must be able to demonstrate effective arrangements to ensure that the use of information complies with legal, regulatory and best practice requirements.

2.4.4 The key principles of Data Quality are Accuracy, Completeness, Consistency, Timeliness, Uniqueness and Validity. This policy will support the Trust in adhering to these principles.



3.0 Process

3.1 **Responsibility and Coverage**

3.1.1 All Staff have a responsibility for data quality and must know and follow Trust procedures relating to data quality management and have attended relevant training or awareness sessions. All staff to be aware of their GDPR responsibilities.

3.1.2 Management - The Chief Executive, Directors and Senior Managers are accountable for data quality within the Trust. Line managers are required to ensure that staff are adequately trained and apply the appropriate procedures and guidelines. Managers are responsible for regularly updating local processes and documents and cascading policy changes to staff. Data Quality must feature in job descriptions of staff with specific responsibilities.

3.1.3 Information Asset Owners (IAOs) should be identified for each electronic or manual system. The IAO is responsible for the quality of data on their system and compliance with relevant legislation and NHS standards.

3.1.4 All Staff must follow Trust procedures for recording data in an accurate and timely manner via paper based or electronic means.

3.1.5 Information Management Staff (Business Intelligence Team) must approve system implementation (i.e., purchase of new systems with reporting requirements) in the Trust in order to minimize development of independent databases and ensure that data quality is part of the design. All data reports and returns to external bodies should be co-ordinated by the Business Intelligence team or authorised personnel so that data quality can be validated prior to submission and to ensure all reports are suitably anonymised to cover information governance risk.

3.1.6 A Data Governance Framework is being introduced to support staff in understanding data quality. There will be tools that can be used to ensure Governance around Data Quality and guidelines in place to make sure a standard approach is used when producing reports.

3.2 Manual Data Input

3.2.1 At the point of collection, staff must validate (using agreed locally procedures) the data they collect from patients, staff and the general public.

3.2.2 Clinical audit information produced for reporting purposes must be validated for accuracy and consistency.

3.3 Computerised Data Input

3.3.1 IAOs must ensure that electronic information assets they are responsible for have inbuilt 'logical checking programmes and input validation rules' that support the accurate collection of information.

3.3.2 IAOs will implement regular system audits and reports to ensure the accuracy of information on their electronic information assets. Localised action plans will be developed by the IAO in relation to any non-compliance issues found.

3.4 Improving Data Quality

3.4.1 The drive to improve and maintain the quality of the Trust's corporate and patient related information is underpinned by a range of initiatives:

- Regular validation of patient care record at point of submission
- Production of data quality reports to identify and enable correction of missing data items and errors on a regular basis
- Monitoring of data quality reports produced so they are of sufficient quality and actions are followed up
- Attendance at local information forums to share local and national issues concerning the collection, recording and submission of corporate and patient related data
- Ensure Business Intelligence (BI) Standard Operating Procedures (SOPs) are followed when producing any performance related data across all service lines e.g. 999, 111 and PTS. The SOPS are stored on Pulse
- Any changes to BI SOPs need to be signed off by the relevant lead for the service line.
- Standard Operating Procedures should be created for the collection and inputting of data where appropriate and the data quality principles should be applied by the relevant information owner

3.5 **Use of the NHS Number**

3.5.1 All NHS organisations are required to improve patient safety by making effective use of the Personal Demographics Service (PDS) and enabling consistent use of the NHS Number to reduce the number of data quality issues due to mis-associated records.

3.5.2 The Trust makes appropriate use of the NHS Number wherever possible in so far as current systems allow.

3.6 **Adherence to GDPR**

3.6.1 The general principles of GDPR to which the Trust must adhere are set out below. These include documenting of a lawful basis for data processing activities and ensuring limiting the processing of data relative to its intended purpose.

1.	**Lawfulness, fairness & transparency**	Personal data must be processed lawfully, fairly and in a transparent manner.
2.	**Limited lawful purpose**	Personal data must be only collected and processed for specified, explicit and legitimate purposes.
3.	**Data minimisation**	Personal data must be adequate, relevant and limited to what is necessary in relation to the intended purpose.
4.	**Accuracy**	Personal data must be accurate and, where necessary, kept up to date.
5.	**Storage limitation**	Personal data must not be kept in a form which permits identification for any longer than necessary for the given purpose.
6.	**Integration & confidentiality**	Personal data must be processed in a manner which ensures its appropriate security.
7.	**Accountability**	The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

4.0 Training Expectations of Staff

4.1 Training and development of staff is key to the achievement of high levels of data quality. The following principles should be met to achieve this:

- All new staff that are to use paper based and electronic information systems will receive appropriate training in the use of the respective systems from appropriate trainers, following approved training plans and learner outcomes. This will include Information Governance induction and mandatory training, as included in the Trust's Training Needs Assessment in the Statutory and Mandatory Training Policy.
- Access to these paper based and electronic information systems will only be issued once the individual has completed the relevant training course and signed off as competent.
- Training must be backed up by regularly reviewed procedures. These should be properly documented and accessible to all appropriate staff. Staff should be made aware of where these are stored and how to access them.

4.2 The Trust will support the development of suitable training courses or materials for appropriate staff to increase awareness of the requirement for accurate data and to undertake the procedures necessary to achieve this.

5.0 Implementation Plan

5.1 The latest approved version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted on how to find and access the policy library during Trust Induction.

6.0 Monitoring Compliance with this Policy

6.1 A yearly internal audit will take place on the Integrated Board Report and related support services who supply data to the Business Intelligence Team.

6.2 Data quality related incidents with an information governance impact will be reviewed by the Information Governance Working Group or Incident Review Group where there has been moderate or above impact on personal identifiable information.

6.3 The IAO information risk review process will prompt IAOs to ensure processes are in place to support the accuracy of information assets and data flows including service user information.

6.4 IAOs will assess the accuracy of data according to the defined standards of the service and will provide feedback to the staff involved through audit arrangements established within the service in order to uphold data quality.

6.5 The Data Security and Protection Toolkit submission will include mandatory compliance statement and supporting evidence for the assertion relating to Data Quality requirements.

6.6 Data quality will be subject to control processes within the Trust and will be subject to external scrutiny:

- **Information provided internally**: Locally defined measures will be used by the Trust to monitor quality. Internal monitoring reports will be used to inform management, improve processes and documentation, and identify training needs. Internal audits will be carried out on systems, processes and data quality to ensure continued compliance with Trust standards.
- **Information provided externally**: Where external agencies receive or have access to Trust information and produce data quality reports and indicators, the Trust will aim to achieve 100% accuracy and completeness on all items.

7.0 References

NHS Records Management – Code of Practice
Records Management Code of Practice - NHS Transformation Directorate

8.0 Appendices

8.1 This Policy includes the following appendices:

Appendix A - Definitions and Explanation of Terms
Appendix B - Roles & Responsibilities

Appendix A - Definitions and Explanation of Terms

This section provides staff members with a high-level overview of definitions and explanations of terms used within this policy:

- **Data** are numbers, words or images that have yet to be organised or analysed to answer a specific question.
- **Information** is produced through processing, manipulating and organising data to answer questions.
- **Knowledge** is what is known by a person. It involves interpreting information received, adding relevance and context to clarify the insights the information contains.
- The **Information Asset Register** provides an inventory of all the business critical electronic and paper-based assets (and those holding person identifiable information) that the Trust holds.

Appendix B - Roles & Responsibilities

Information Asset Owner (IAO)

All IAOs have responsibility for data quality (delegated authority of the Senior Information Risk Owner – SIRO). The IAOs are nominated leads for information assets and have the responsibility for monitoring the day-to-day management of data quality in respect of electronic and paper records, ensuring the importance of data quality is upheld within their area of responsibility. All electronic and paper records will be the responsibility of the IAOs. All IAOs are responsible for developing appropriate procedures to ensure the accuracy of the data held within their systems and processes and timeliness of necessary corrections to that data.

Business Intelligence Team

The Business Intelligence team are responsible for checking and assuring the quality of the information they produce however, recipients of scheduled weekly or monthly information should check all reports for inconsistency of information or missing data. All errors and anomalies should be reported to the Business Intelligence team for investigation and corrective action taken as soon as possible.

The appropriate department or individual will investigate queries, gaps in data items, and anomalies raised by the Business Intelligence team as a result of report production. Errors and omissions will be corrected within agreed timescales.

External data reports, such as those produced by Adastra or MIS, will be checked by the Business Intelligence team and any issues addressed prior to the next return deadline.

Information Governance Working Group (IGWG)

The IGWG will monitor the effectiveness of the corrective actions in respect of Information Governance incidents are implemented.

All Staff

Who are involved with the collation, recording, extraction, analysis of data have a responsibility to ensure it is of the highest quality at the point of capture and are familiar and comply with, local data quality procedures and relevant legislation.