



# Data Quality Policy

**Document Author: Business Intelligence Manager**

**Date Approved: June 2016**



<b>Document Reference</b>	PO – Data Quality Policy – June 2018
<b>Version</b>	4.1
<b>Responsible Committee</b>	Trust Management Group
<b>Responsible Director (title)</b>	Director of Finance & Performance
<b>Document Author (title)</b>	Business Intelligence Manager
<b>Approved By</b>	Trust Management Group
<b>Date Approved</b>	June 2016
<b>Review Date</b>	June 2018
<b>Equality Impact Assessed (EIA)</b>	Yes
<b>Protective Marking</b>	Not Protectively Marked

### Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
2.0	March 2007	David Johnson Assistant Director of IM&T	A	
2.1	February 2014	Stephen Graham Business Intelligence Manager & Caroline Squires, IG Manager	D	Full Review
3.0	March 2014	Stephen Graham Business Intelligence Manager	A	Approved by the 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
4.1	Feb 2018	Risk Team	D	Document formatting – New Visual Identity
A = Approved D = Draft				
Document Author: Business Intelligence Manager				
Associated Documentation: <ul style="list-style-type: none"> <li>Information Governance Policy</li> <li>Information Governance Strategy</li> <li>Data Protection Policy and Associated Procedures</li> <li>Records Management Policy</li> <li>Health Record-Keeping Standards Guideline</li> </ul>				

<b>Section</b>	<b>Contents</b>	<b>Page No.</b>
	Staff Summary	3
1	Introduction	3
2	Purpose/Scope	4
3	Process: Responsibility and Coverage	4
4	Training Expectations for Staff	6
5	Implementation Plan	6
6	Monitoring Compliance with this Policy	6
7	References	8
8	Appendices	9
	Appendix A – Definitions and Explanation of Terms	9
	Appendix B – Roles and Responsibilities	10

## Staff Summary

Everyone who is involved in the collection and recording of information, including service user information, is responsible for ensuring its accurate collection in order to minimise risks to the service user and to the organisation.

High quality information means better care and safety. If service user information is inaccurate, there could be consequences for care, treatment and safety.

Information Asset Owners (IAO's) are responsible for ensuring documented procedures and processes are in place to ensure the accuracy of information including service user information on all systems and/or records, including those that support the provision of care.

IAO's are responsible for ensuring adequate training is provided to staff to ensure the accurate collection of information, including service user information and onward reporting of high quality information.

### 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.

### 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 Information Governance. This policy will be support by a data quality strategy

### **3.0 Process: Responsibility and Coverage**

- 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.
- 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.
- IAOs should be identified for each electronic or manual system. The owner is responsible for the quality of data on their system and compliance with relevant legislation and NHS standards.
- Clinical Staff must follow Trust procedures for recording data in an accurate and timely manner via paper based or electronic means.
- 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.

#### **3.1.1 Manual Data Input**

- At the point of collection, staff must validate (using agreed locally procedures) the data they collect from patients, staff and the general public.
- Clinical audit information produced for reporting purposes must be validated for accuracy and consistency.

#### **3.1.2 Computerised Data Input**

- 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.
- 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.

#### **3.1.3 Improving Data Quality**

- The drive to improve and maintain the quality of the Trust's corporate and patient related information is underpinned by a range of initiatives:
  - a. Regular validation of patient care record at point of submission;
  - b. Production of data quality reports to identify and enable correction of missing data items and errors on a regular basis;
  - c. Monitoring of data quality reports produced so they are of sufficient quality and actions are followed up;

- d. Attendance at local information forums to share local and national issues concerning the collection, recording and submission of corporate and patient related data;
- e. Supporting compliance and continuous improvement against the Trust's Information Governance Toolkit submission (IG Toolkit 'Clinical Information Assurance Management') .

#### **3.1.4 Use of the NHS Number**

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

#### **3.1.5 Improving Effectiveness of Data Quality**

##### **Adherence to Data Quality Principles**

Although there are many aspects to good data quality, the general principles that the Trust must adhere to are as follows:

##### **Validity**

- All data items held on the Trust computer systems should be valid. Where codes are used, then these should comply, where possible and applicable, with national standards. System applications should include functionality to error trap invalid input where this is possible.

##### **Completeness**

- All internally agreed data items within a data set should be completed. Data fields for national requires will be declared as mandatory in Trust applications where possible. Default codes will only be allowed when appropriate and should not be used as a substitute for actual data. If it necessary to bypass a data item in order to treat a service user then the missing data must be reported for immediate follow up.

##### **Reliability**

- Data items should reliable and internally consistent. For service users with multiple episodes, recorded dates should be consistent and where multiple referrals or episodes exist, interventions should be linked correctly. Clinical coding should be consistent for ages and sex.

##### **Coverage**

- Data will reflect all clinical, operational and managerial work carried out by the Trust staff. Procedures will be put in place to ensure complete data capture where possible. Spot checks, exception reports and audits will be utilised to identify missing data.

##### **Accuracy**

- Manual and electronically held data should accurately reflect each other and the care and treatment provided to the service user.
- All reference data should be updated regularly with procedures in place to ensure that updates are implemented in a timely manner.

- Every opportunity should be taken to ensure that demographic details are checked with the service users themselves.

### **Timeliness**

- All data must be recorded within agreed specified deadlines. For computer applications, best practice dictates that data entry should take place at, or as near as possible to, an event being recorded. This will ensure the safe and effective care and treatment of service users. Additionally, it will ensure that up to date data can be included in national, local and internal reports.

### **Anonymity**

- All patient level data not being used for direct patient care, must be anonymised or pseudonymised to protect patient confidentiality.

## **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 their line managers. 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 training has been completed to the satisfaction of the line manager.
- 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 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 this policy 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 information governance incidents will be monitored by the Information Governance Working Group.

6.3 Via the quarterly IAO information risk review process the Information Governance Manager will monitor that IAOs are ensuring documented procedures and processes

are in place to support the accuracy of information including service user information on all systems and/or records including those that support the provision of care.

- 6.4 IAOs and the IG Manager will provide progress reports to the Information Governance Working Group (IGWG) and areas of non-compliance will be monitored by the group.
- 6.5 IAOs will monitor performance in collecting data according to the defined standards and provide feedback to the staff involved in the data collection process.
- 6.6 The Department of Health Information Governance Toolkit requires the Trust to undertake self-assessment based upon defined indicators, the Trust is regularly audited to ensure that the suitable processes, controls and legislative Acts are complied with.
- 6.7 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

- 7.1 NHS Records Management – Code of Practice Part 1  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/200138/Records\\_Management\\_-\\_NHS\\_Code\\_of\\_Practice\\_Part\\_1.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200138/Records_Management_-_NHS_Code_of_Practice_Part_1.pdf)
- 7.2 NHS Records Management – Code of Practice Part 2  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/200139/Records\\_Management\\_-\\_NHS\\_Code\\_of\\_Practice\\_Part\\_2\\_second\\_edition.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf)
- 7.3 The Health and Social Care Information Centre NHS Information Governance Toolkit  
<https://nwww.igt.hscic.gov.uk/>

## 8.0 Appendices

### 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 staff or patient identifiable information) that the Trust holds.

## Appendix B - Roles & Responsibilities

- **IAO** – All IAO's have responsibility for data quality (delegated authority of the Senior Information Risk Owner – SIRO). The IAO's 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 Information Asset Owners (IAO's). All IAO's 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.
- **Information Governance Manager** - Within the Standards and Compliance Directorate, the information Governance Manager, has the specific aim of promoting data quality best practice within the Trust.
- **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 Department 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 implemented where non-conformity has been identified.
- **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.