Arthington Medical Centre

5 Moor Road, Hunslet, Leeds, LS10 2JJ
0113 385 2180

DATA QUALITY POLICY

Review and Amendment Log / Control Sheet

Author:	West Yorkshire ICB Senior Information Governance Officer
Date Approved:	April 2023
Approved by:	Mena Suri
Version:	1.0
Review Date:	April 2025

Version History

Version no.	Date	Author	Status	Circulation
1.0	April 2023	Senior IG Officer	Approved	All Practice Staff

Executive Summary

This Policy sets out the way the practice wishes to ensure a consistent approach to Data Quality, in support of legislative, regulatory, statutory, and business requirements.

Data Quality is defined within this policy as the; accuracy, validity, reliability, timeliness, relevance, completeness and robustness of data. Everyone who is involved in the collection and recording of information is responsible for ensuring its accurate collection in order to minimise risks to the organisation or individuals.

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 in addition to being 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.

Equality Statement

This policy applies to all employees, Managing Partnership members and members of Arthington Medical Centre irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION....5

2. AIMS....5

3. SCOPE....6

5. ACCOUNTABILITY AND RESPONSIBILITIES....8

6. DEFINITION OF TERMS....8

6. GENERAL GUIDELINES AND PRINCIPLES OF DATA QUALITY....8

7. EXTERNAL SOURCES OF DATA....10

8. PROCEDURE FOR DATA QUALITY MANAGEMENT....10

9. TRAINING....11

9.1 Mandatory Training....11

9.2 Specialist Training....11

10. IMPLEMENTATION AND DISSEMINATION....11

11. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY....11

12. ADVICE AND GUIDANCE....12

13. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)....12

14. OTHER LEGISLATION AND GUIDANCE....13

15. GLOSSARY....15

1. INTRODUCTION

Arthington Medical Centre recognises that all their decisions, whether health care, managerial or financial need to be based on information which is of the highest quality. Data quality is crucial, and the availability of complete, accurate, relevant and timely data is important in supporting patient care, governance, management and service agreements for health care planning and accountability.

The Practice aspires to the highest standards of clinical competence and corporate behaviour to ensure that safe, fair, and equitable procedures are applied to all organisational transactions, including relationships with patients their carers, public, staff, stakeholders, and the use of public resources.

The importance of having robust systems, processes, data definitions and systems of validation in place to assure data quality is part of this process. The quality of data can affect the reputation of the Practice and may lead to financial penalty in certain circumstances, e.g., failing to meet contractual requirements, QoF expectations and other reportable outcome measures.

The purpose of this policy is to provide general principles for the management of all data and guidance. This is to ensure that the Practice can take decisions based on accurate and complete data and can meet its various legal and regulatory responsibilities.

A data quality policy and regular monitoring of data standards are a requirement of the NHS Data Security Protection Toolkit

Information accuracy is also a legal requirement under the GDPR/Data Protection Act 2018

This policy provides the framework to mitigate against the risk of poor data quality and enable individuals within the Practice to take direct responsibility for any data they record or omit to record.

2. AIMS

Ever-increasing use of computerised systems provides greater opportunities to store and access large volumes of many types of data but also increases the risk of misinformation if the data from which information is derived is not of good quality.

This risk applies to information for the Practice’s internal use and to information conveyed in the form of statutory returns to the national databases.

For our information to have value, it is essential that the underlying data is consistent and complies with national standards. NHS Practices are assessed, judged and sometimes paid for on the quality of the data they produce.

National statistics, performance indicators and audit assessments depend on good quality data for their accuracy and include data quality amongst their number.

The Data Quality Policy underpins the practice's objective to record and present data of the highest possible quality and that all users of the information can be confident about its accuracy.

The Practice will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the UK GDPR and the DPA 2018 and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Protection and Security Toolkit (DSPT).

This policy supports the Practice in their role as providers of health services and will assist in the safe sharing of information with partners and agencies.

3. SCOPE

This policy must be followed by all staff who works for or on behalf of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy is applicable to all data held and processed by the Practice.

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.

Written procedures will be available in all relevant locations within the Practice to assist staff in collecting and recording data. These procedures will be kept up-to-date, and where appropriate will also contain information relating to national data definitions.

Processes will be established to ensure compliance with the procedures, which will include sample checks to audit compliance.

It should be noted that all collection, storage, processing and reporting of personal information is governed by detailed legal requirements under the GDPR/Data Protection Act 2018 and associated standards, such as the Caldicott guidelines and Health and Social Care Act 2012

As the Practice generates a very wide range of information for a whole variety of uses, this policy does not provide detailed guidance for specific data items or individual areas of application. It concentrates instead on general principles of completeness, accuracy, ongoing validity, timeliness, consistency of definitions and compatibility of data items, and signposts where specific procedures or further guidelines need to exist.

- 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, including external partners is of the highest quality.

- Business planning – ensuring management can rely on the information to make informed and effective business decisions.

- The measurement of activity and performance to ensure effective distribution and use of Practice resources.

- Regulatory reporting – to ensure compliance with the standards and targets as laid down in measures such as QoF, DSP toolkit etc.

- Good corporate governance – which, as above, has data quality as a pre-requisite to ensure effective business management.

- Legal compliance – ensuring that the Practice conforms to its legal obligations as laid down in relevant legislation, such as GDPR/Data Protection Act 2018.

Education and Training – in the development and delivery of quality education and training provision.

5. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key information governance roles and bodies that the Practice needs to have in place as part of its Information Governance Framework, these are:

- Data Protection Officer (DPO)
- Managing Partnership
- Governance, Performance and Risk Committee
- Caldicott Guardian
- Information Asset Owner (IAO)
- Information Asset Administrator (IAA)
- Heads of Service/department
- All employees

6. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

Please refer to the glossary of terms within this policy.

6. GENERAL GUIDELINES AND PRINCIPLES OF DATA QUALITY

Supplying accurate data is a complicated task for a few reasons:

- There are many ways for the data to be inaccurate – data entry errors and incomplete data, etc.

- Data can be corrupted during translation depending on who is translating it, how and with what tools/processes.

- Data must relate to the correct time period and be available when required.

- Data must be in a form that is collectable and which can subsequently be analysed.

To ensure an organisation achieves data quality, it must set out how :

- Data is collected and co-ordinated.
- Data is transferred between systems.
- Data is organised.
- Data is analysed.

- Data is interpreted.
- Conclusions and results drawn from the data are validated.

The following overarching principles underpin the approach to data quality:

- All staff will conform to legal and statutory requirements and recognised good practice, aim to be significantly above average on in-house data quality indicators, and will strive towards 100% accuracy across all information systems.

- All data collection, manipulation and reporting processes by the Practice will be covered by clear procedures which are easily available to all relevant staff, and regularly reviewed and updated.

- All staff should be aware of the importance of good data quality and their own contribution to achieving it and should receive appropriate training in relation to data quality aspects of their work.

- Teams should have comprehensive procedures in place for identifying and correcting data errors, such that information is accurate and reliable at time of use.

Data can be said to be of ‘high quality’ if the data accurately portray exact details and/or events that took place- the following principles should be considered when doing so.

- **Accessibility**
  Information can be accessed quickly and efficiently using systematic and consistent management in electronic (and physical) format. Access must be appropriate so that only those with a lawful basis and legitimate relationship to the data may view, create, or modify them.

- **Accuracy**
  Data (and information) are accurate with systems, processes, and practice in place to ensure this. Any limitations on accuracy of data must be made clear to its users and effective margins of error need to be considered for calculations.

- **Completeness**
  Completeness can have a real impact on the quality of data. The evaluation of data quality must monitor for missing, incomplete, or invalid information as well as identification of future or occurring causes and the associated risks.

- **Relevance**
  Data captured should be appropriate for the intended purpose and never excessive.

- **Reliability**
  Data and information must reflect a stable, systematic, and consistent approach to enhance reliability. Review and enforcement of collection methods of data must be considered to ensure a positive impact on the quality or content of any information produced.

- **Timeliness**
  Data should be recorded as close as possible to being gathered and should be accessed quickly and efficiently, in line with Data Protection legislation and guidance.

- **Validity**
  Validity is supported by consistency over time, systems and measures; data must be collected, recorded and utilised to the standard set by relevant requirements or controls. Any information collection, use or analytical process must incorporate an agreed validation method or tool to ensure the standards and principles outlined above are met. Validation tools will support routine data entry and analysis, as well as supporting the identification and control of duplicate records and other errors.

7. EXTERNAL SOURCES OF DATA

Where possible validation processes should use accredited external sources of information e.g., using Patient Demographic Service (PDS) to check NHS numbers. Staff involved with recording data need to ensure that it is performed in a timely manner and that the details being recorded are checked with the source at every opportunity.

The NHS number is the main patient identifier and must be recorded correctly and, in all systems, where patient information is present. The NHS number should be used in all referral forms and letters. The Data Security and Protection Toolkit requires evidence outlining the NHS number is used and there is a mandatory NHS number field in all documentation and systems.

8. PROCEDURE FOR DATA QUALITY MANAGEMENT

Individuals listed in the “Accountability and Responsibilities” section will adhere to published procedures, or standard operating procedures, as indicated to discharge this policy in their domain.

9. TRAINING

9.1 Mandatory Training

The Data Security Protection Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance in accordance with the IG Training Strategy.

Line managers must actively ensure that all staff undertake and complete the annual mandatory information governance training.

9.2 Specialist Training

Additional training may be provided in specialist areas such as data protection. The need for additional training should be identified with reference to the IG Training Strategy.

General Clinical System training offered to all staff.

Training issues with systems and/or other specific processes should be addressed on an individual basis as they arise.

10. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Practice's IG/Management Team   this policy will be disseminated to staff via an appropriate medium e.g., the Practice's Intranet or communication through in-house staff briefings.

This Policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

11. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

To be assured that this policy is being implemented, key elements will be monitored for compliance.

- Compliance with the mandatory assertions of the Data Security and Protection Toolkit.

- All staff receive annual training and competency test in Data Security Awareness.

- All Information Asset reviewed annually. New information assets will be identified through this review process.

- Statistically validated reduction in Information Governance related incidents.

Data quality is ultimately the responsibility of department leads where the specific data are being generated. Processes for ensuring high data quality will differ between teams and should be implemented and reviewed locally.

12. ADVICE AND GUIDANCE

Advice and guidance on any matters stemming from the Policy can be obtained by contacting the West Yorkshire ICB Information Governance Team: wyicb-leeds.dpo@nhs.net

13. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

This policy should be read in conjunction with:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Mobile Working Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and Social Media Policy
- Email Policy

And their associated procedures (including but not limited to):

- Subject Access Request (Access to Health Records) Procedure
- Information Sharing Protocol
- Freedom of Information Procedures

- Data Protection Impact Assessment Procedure and supporting documents
- Safe Transfer Guidelines and Procedure

This policy should also be read in conjunction with the Information Governance Handbook which provides guidance for staff on information governance compliance.

14. OTHER LEGISLATION AND GUIDANCE

- The Abortion (Amendment) Regulations 2022
- Access to Health Records Act 1990 Health and Social Care Act 2012
- Audit and Internal Control Act 1987
- Bribery Act 2010
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Enterprise and Regulatory Reform Act 2013
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- UK General Data Protection Regulation and Data Protection Act 2018
- Health and Social Care Act 2012
- Health and Social Care (Quality and Safety) Act 2015
- Health Service (Control of Patient Information) Regulations 2002
- Human Rights Act 1998
- Information Commissioner's Guidance Documents
- ISO/IEC 27001:2005 Specification for an Information Security Management system
- ISO/IEC27002:2005 Code of Practice for Information Security Management
- National Data Guardian's Ten Data Security Standards
- NHS Act 2006
- NHS Information Security Management Code of Practice 2007
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Professional Codes of Conduct and Guidance
- Protection of Freedoms Act 2012

- Public Records Act 1958
- Public Interest Disclosure Act 1998
- Regulation of Investigatory Powers Act 2000 (Lawful Business Practice Regulations 2000)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992

This is not an exhaustive list and further guidance can be obtained from the Information Governance Team.

15. GLOSSARY

Term Used	Definition of word or phrase
Bulk transfer of person identifiable or sensitive data	Used to describe information relating to 21 or more individuals.
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Consent	The consent of the 'data subject' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
Data Breach	Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Data Controller	Data Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor	Processor means a natural or legal person, public. authority, agency, or any other body which processes personal data on behalf of the controller.
Data Protection Officer (DPO)	The DPO is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance which includes conducting assurance audits.
Data Subject	An identified or identifiable 'living individual' whose personal data is processed by a controller or processor. Otherwise known within data protection legislation as a 'natural person'.

Term Used	Definition of word or phrase
Declaration	Declaration is the point at which the document (i.e., the record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Document	The International Standards Organisation (ISO) standard 5127:2017 now states 'recorded information shall be treated as a unit in a documentation process regardless of its physical form or characteristics'.
Electronic document	Information recorded in a manner that requires computer or other electronic device to display, interpret and process it. This includes documents (whether text, graphics, or spreadsheets) generated by software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in Electronic Data Interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.
Encryption	The process of transforming information (referred to as plain text) using an algorithm (called 'cipher') to make it unreadable to anyone except those possessing special knowledge, usually referred to as a 'key'.
File Plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet the records management needs.
Folder	A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable). Folders are allocated into a class.

Term Used	Definition of word or phrase
Health Record	Information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual.
Information Asset Owners (IAOs)	Are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’. Information Asset Owners may be assigned ownership of several information assets.
Information Asset Register	Is a list of information assets owned by the Practice.
Information Assets	Are operating systems, infrastructure, business applications, off the shelf products, services, user- developed applications, records, and information.
Information lifecycle management	Information lifecycle management is the policies, processes, practices, services, and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Records Management policies and procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage, records audit etc.
Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Mobile Computing	Covers the use of portable computing devices, such as laptops, mobile phones, tablet computers, memory sticks or equivalent mobile computing equipment.

Term Used	Definition of word or phrase
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record, or folder.
Network	A system that connects two or more computing devices for transmitting and sharing information. Inclusive of all components processing data at organisations point of entry and excludes any end user devices connecting to a switch, hub or wireless access point or any systems monitoring network devices.
Network File Server	Is computer hardware with large storage capacity which? is held in a highly secure area.
Personal Data	Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier, including (but not limited to): • Name • Date of Birth • Post Code • Address • National Insurance Number • Photographs, digital images etc. • NHS or Hospital/Practice Number • Location data Personal data that has been pseudonymised can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.
Processing	Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Term Used	**Definition of word or phrase**
Pseudonymisation	Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each identifiable patient data item. It enables NHS organisations to undertake secondary usage of patient data in a legal, safe, and secure manner.
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (the ISO standard, ISO 15489-1:2016 Information and documentation - records management).
Records Management	The process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.
Responsible User	Individual members of staff who personally adhere to the Practice’s IT Security Policy (incorporating Network Security) and make use of the computer facilities provided to them by the Practice in an appropriate and responsible fashion.

Term Used	Definition of word or phrase
Safe Haven	A term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the Practice whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles.
Senior Information Risk Owner (SIRO)	The SIRO is a senior officer of the Practice. The SIRO acts as an advocate for information risk for the Practice and leads and implements the information risk assessment programme.
Special Category Data	Special Category Data (or sensitive personal data) are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Subject Access Right	Entitles the data subject to have access to and information about the personal data that a controller has concerning them. Also known as the Right of Access.
Users (end users)	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much or the material which constitutes the record. Since records systems tend to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.