NHS

Walsall Clinical Commissioning Group

Data Quality Policy

Data Quality Policy
For
Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 05 March 2019
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V1.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	05 March 2019
Date Policy is Effective From	Date of ratification
Review date:	January 2020
Expiry date:	March 2020
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff and staff working for the CCG
National Documents	
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation

Circulated to the following for consultation

Name/Committee/Group/	Designation

IG Function Leads	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author

Contents

1 Scope

The purpose of this policy is to reinforce Walsall Clinical Commissioning Group's (CCG) commitment to data quality. Good data quality ensures good information. The policy will provide staff working in every area with guidelines as to their roles and responsibilities in respect of data quality.

The scope and principles set out in this policy are applicable to all information held in hard copy or electronically including both clinical and administrative.

This policy applies to:

- All information that is held in hard copy or electronically whether centrally or locally maintained
- The development and implementation of any new data capture and storage processes hard copy or electronically
- All staff employed by or working on behalf of the CCG who collect, use, input or report on information contained within the CCG's information systems

Failure to follow the requirements of this policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the CCGs disciplinary or capability policies and procedures.

2 Introduction

Reliable information is a fundamental requirement for the CCG to conduct its business efficiently and effectively. This applies in all areas of activity including the delivery of care, service management, performance management, corporate governance, internal and external accountability and communication. Data is used to manage and improve the ways in which the CCG achieves its business objectives. Data quality is therefore a crucial pre-requisite to information that is complete, relevant, accurate and timely.

Poor data quality may lead to:

- Staff and patients being put at risk through invalid or incorrect decisions being made
- Vulnerable people put at risk through missing data leading to possible mistaken identity or missed alarms about an individual or quality of care
- Lack of confidence in the validity of the recorded/reported information
- Poor management decisions relating to the CCG both internally and externally
- Loss of credibility of the organisation

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

In order to achieve and maintain a high level of quality data it is important that the CCG puts in place processes for assessing, measuring, reporting, reacting to and controlling the risks associated with poor data quality. The aim of this policy therefore is to provide the framework for establishing, maintaining and improving the quality of data across the CCG. Data can only be regarded as fit for purpose if it is:

- Valid
- Complete
- Consistent
- Accurate and up to date
- Relevant
- Available when required
- Secure in compliance with Data Protection Act and Caldicott Guidelines

3 Status

This policy is an Information Governance policy.

3.2 Purpose and scope

This policy is designed to ensure that the importance of data quality within the CCG is disseminated to all staff. It will describe the meaning of data quality, who is responsible for its maintenance and how it can continue to improve in the future.

Although this policy relates to patient/service user data and information, the principles included are applicable to any other data/information staff may encounter i.e. recording of minutes, etc.

4. Definitions

4.1 Data: Data is a collection of facts from which information is constructed via processing or interpretation

4.2 Information: Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver

4.3 Data Quality: Data quality is a measure of the reliability of data for any purpose

4.4 Data Protection Act 2018: The provisions detailed within the Act provide the statutory guidance for the protection and use of personal information

4.5 Information Assets The primary information systems used for the capture and maintenance of data within the CCG

4.6 Information Asset Owner (IAO) The individual with responsibility for the management of an information system

4.7 Information System Administrator (IAA) The individual with responsibility for the day to day administration and operation of an information system

4.8 Data Security and Protection Toolkit This provides a framework for assuring information quality requiring the monitoring of key data items against national definitions

5 Roles and Responsibilities

Data quality is the responsibility of everyone in the CCG who collects and uses data, however there are a number of different roles and groups which have some key responsibilities for data quality in the CCG.

5.1 Chief Officer

The Chief Officer is the lead on the Governing Body for Information Governance.

5.2 Governing Body

It is the role of the Governing Body to define the CCG's policy in respect of Information Governance, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.3 Chief Financial Officer (Senior Information Risk Owner)

The CCGs Chief financial officer is the Senior Information Risk Owner (SIRO). The role of the SIRO is to take ownership of the organisations information risk policy, act as an advocate for information risk on the Governing Body and provide written advice to the Accountable Officer on the content of the annual governance statement in regard to information risk.

5.4 Medical Director (Caldicott Guardian)

Responsibility for ensuring that all patient related personal data is processed and managed in accordance with the Caldicott Principles. The Medical Director acts as the CCGs Caldicott Guardian with responsibility for patient confidentiality.

5.5 Data Protection Officer

The CCG have appointed a Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with others to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, Data Protection Impact Assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

The Data Protection Officer has assumed the below duties in compliance with GDPR Article 39: -

- To inform and advise the CCG and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions
- To monitor compliance with the GDPR, associated data protection provisions and THE CCGs own data protection policies, procedures and objectives
- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training program
- To co-operate with the Supervisory Authority where required
- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the DPO will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant
- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing
- The above-mentioned policies, procedures, employee duties and training programs

5.6 Information Governance Operational Group

The Information Governance Operational Group IGOG purpose is to support and drive the broader information governance agenda. The group will make recommendations to the Audit & Governance Committee and provide assurance that the CCG is compliant with IG requirements.

5.7 Information Asset Owner (IAO)

The same principles covered in this policy apply to all systems where managed centrally or by individual information system owners and are responsible for:

- Maintaining data standards in accordance with national and/or system developments in relation to the system for which they are responsible
- Ensuring that the system facilitates the collection of high quality data in accordance with national/local standards
- Monitoring and disseminating changes
- Establishing and disseminating monitoring reports from the system to appropriate staff and service detailing key data quality issues
- Reporting any concerns to the appropriate manager
- Ensuring that any data quality issues are reflected in any directly related individual system documentation
- Logging any information security issues relating to data quality with the Information Governance Department
- Logging any data quality issues, where appropriate

5.8 All staff working within the CCG

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

All staff including temporary or agency staff in conjunction with their line manager are responsible for:

- Implementing and maintaining data quality and are obligated to maintain accurate information legally (Data Protection Act 2018) (GDPR and UK Data Protection Bill from 25 May 2018), contractually (contract of employment).
- Compliance with relevant policies. Failure to comply may result in disciplinary action being taken.
- Co-operating with the development and implementation of policies and as part of their normal duties and responsibilities.
- Ensuring the timely accurate and complete input of data onto the appropriate CCG information system or data recording sheets.
- Ensuring that they have the appropriate level of knowledge and skills for using the information systems.
- Undertake regular validation checks of data collection and input to confirm that the data for which they have responsibility for is accurate, complete and up to date.
- Monitoring the data held for any data quality issues and reporting any concerns to the

appropriate information asset owner.

- Identifying the need for a change in policy as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local or national directives and advising their line manager accordingly
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training and awareness sessions as required or completing training materials when provided.

6. Data Quality

6.1 Importance of Data Quality

6.1.1 Having accurate, relevant information that is accessible at the appropriate times is essential to each and every health management or business decision and to the success of the service provided. With this in mind, it is essential that all employees of the CCG recognise the importance of data quality and their responsibilities in this area.

6.1.2 Quality information is essential for:

- The delivery of effective, relevant and timely care, and to minimise risks to patients.
- Efficient administrative and health care processes, such as communication with patients, their families and other carers and professionals involved in their treatment/care.
- Management and strategic planning, requiring accurate information about the volume and type of health care activity to provide appropriate allocation of resources and future service delivery.
- Establishing acceptable service agreements for health care provision.
- Health care governance, which depends on detailed, accurate patient data for the identification of areas where health care could be improved.
- Providing information for other NHS and non-NHS organisations – these organisations depend on the information we send them and need to have confidence in its quality.
- Providing a foundation on which future investments will be based, such as the implementation of the National Programme for IT, where data will be shared on the spine and accessed by other parts of the NHS.
- Being able to allow local and national benchmarking.
- Budget Monitoring, including Payment by Results, and financial planning to support service delivery.
- Avoiding unnecessary Subject Rights Requests to alter incorrect personal data

6.1.3 It is also important to ensure that the data quality is of a high standard in order to comply with the Data Protection Act 2018 in particular principle 4, 'accurate and up-to-date' and to satisfy the data quality requirements within the NHS Care Record Guarantee.
6.1.4 From 25 May 2018 the Data Protection Legislation in the UK incorporates the EU General Data Protection Regulations. As well as outlining 6 principles of data protection, the new legislation contains a new principle of accountability for data controllers and processors and introduces new rights for data subjects, one of which is the right to have incorrect personal data amended.

6.2 Data Standards

6.2.1 The standards for good data quality are reflected in the criteria below. Data needs to be:

- Complete (in terms of having been captured in full)
- Accurate (the proximity of the data to the exact or true values)
- Relevant (the degree to which the data meets current and
- potential user's needs)
- Accessible (data must be retrievable in order to be used and in order to assess its quality)
- Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised national and local standards)
- Defined (understood by all staff who need to know and reflected in procedural documents)
- Appropriately sought (in terms of being collected or checked with the patient during a period of care)
- Appropriately recorded (in both paper and electronic records)
- Processed in accordance with any existing data sharing agreement of data processing agreement.

6.2.2 The use of data standards within systems can greatly improve data quality. These can be incorporated into systems either using electronic validation programmes which are conformant with NHS standards, e.g. drop down menus, or manually generated lists for services that do not yet have computer facilities. Either method requires the list to be generated from nationally or locally agreed standards and definitions, e.g. for GP practice codes, ethnicity, etc. These must be controlled, maintained and updated in accordance with any changes that may occur, and in addition electronic validation programmes must not be switched off or overridden by operational staff.

6.2.3 <u>NHS Data Model and Dictionary</u>

Where ever data is captured and stored, reference should be made to the NHS data model and dictionary as this establishes data standards and codes that sets out what should be followed where appropriate.

The NHS Data Model and Dictionary gives common definitions and guidance to support the sharing, exchange and comparison of information across the NHS. The common definitions, known as data standards, are used in commissioning and make up the base currency of Commissioning Data Sets. On the monitoring side, they support comparative data analysis, preparation of performance tables, and data returned to the Department of Health. NHS data standards also support clinical messages, such as those used for pathology and radiology. NHS data standards are presented as a logical data model, ensuring that the standards are consistent and integrated across all NHS business areas.

6.2.4 Changes to the Data Dictionary are announced the following:

- The NHS communicates key changes to data standards, and deadlines affecting changes are made through ISNs. These changes must be monitored by IAOs (system administrators) to ensure that data and information systems to which ISNs apply are in compliance with the standards they specify

- Individual systems IAOs are responsible for gaining assurance that the suppliers of the CCG information systems are updated in accordance with new ISNs to ensure systems conform to all requirements.

- From a commissioning perspective, changes need to be made to the data quality processes to ensure any changes have been implemented by suppliers of data e.g. provider services.

6.2.5 Where no National Standards Exist

In certain situations, there will be no applicable NHS national standards. In these instances, the CCG will agree local standards as part of the contracting process. It is important that any local standards are subject to annual reviews within the CCG as there will be no automatic input received from national sources. This process will ensure their validity and continued relevance.

6.3 Data Validation

6.3.1 Importance of validation

- Validation encompasses the processes that are required to ensure that the information being recorded is of good quality. These processes deal with data that is being added continuously and also can be used on historical data to improve its quality.

- It is imperative that regular validation processes and data checks/audits are undertaken on data being recorded to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include, checking for duplicate or missing data, checking for deceased patients, validating waiting lists, ensuring that national definitions and coding standards are adopted, and NHS number is used and validated.

- Wherever possible, under ther terms of polices WCCG should take steps to ensure that data supplied by Healthcare providers is both valid and complete

6.4 Timescales for validation

Where inconsistencies in data and information are identified these must be acted upon in a timely fashion and documented. Locally agreed deadlines will apply to the required corrections but all amendments should be made within a maximum of two months from the identification date.

Where a data subject is making a Data Rights Request to correct or amend inaccurate data, the process must be completed and the data subject informed within 30 calendar days under Data Protection Legislation.

6.5 External sources of data

Operating within the CCG polices concerning personal identifiable data where possible validation processes should use accredited external sources of information, for example using Patient Demographic Service (PDS) to check NHS numbers

The CCG will use external sources of data to improve data quality, for example, SUS data quality dashboards on a regular basis to check comparative data and identify previously unidentified issues.

6.6 Timeliness of Data Capture

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. This could be by cross checking with patient paper records or by asking the patients themselves.

6.7 NHS Numbers

Operating within the CCG polices concerning personal identifiable data the NHS number is a unique way of identifying patients in NHS systems. With this in mind it is imperative that this is recorded correctly and in all systems where patient information is present.

The Personal Demographics Service (PDS) will be used to obtain verified NHS numbers i.e. NHS number status and as PDS has significant historic data it will enable record matching process and support the resolution of data anomalies (see also External Sources of Data section).

6.8 Monitoring of Data Quality

As a commissioning organisation, the CCG has the responsibility of monitoring the data quality of the services it commissions. This will be carried out in a variety of ways according to the type of service and the data it collects. Examples include, NHS number compliance, pseudonymisation, compliance with new ISNs, Reference Cost Audits, Data Security and Protection Toolkit data quality requirements. The responsible department will report the monitoring of data quality to the responsible committee in accordance with agreed timescales.

7. Implementation

This policy will be available to all Staff for use in relation to the specific function of the policy.

All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

8. Training Implications

The staff responsible for handling data quality in the CCG must have appropriate skills.

All staff working with information systems must be appropriately trained in data quality and the importance it commands for the management and provision of patient care.

9. Related Documents

9.1 Legislation and statutory requirements

- Data Protection Act 2018
- General Data Protection Regulations 2016

9.2 Best practice recommendations

- NHS Digital Data Protection and Security Toolkit – data quality requirements
- NHS Care Record Guarantee

10. Monitoring, Review and Archiving

10.1 Monitoring

The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

10.2 Review

10.2.1 The responsible committee for data quality will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

10.2.2 Staff who become aware of any change which may affect a
policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

10.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'version control' table on the second page of this document.

10.3 Archiving

Please review WCCG's Corporate Records Policy , which makes reference to the Department of Health's Records Management Code of Practice for Health and Social Care 2016.