

Data Quality Policy

Reference No:	IG25
Version:	0.1
Ratified by:	Final
Date ratified:	29 th March 2019
Name of originator/author:	Information Governance, Arden & Greater East Midlands Commissioning Support Unit (AGEM CSU)
Name of responsible committee/individual:	Wendy Martin, Caldicott Guardian NHS Lincolnshire West CCG
Date Approved by committee/individual:	1 st March 2019 – LWCCG Risk & Governance Committee
Date issued:	February 2019
Review date:	February 2022
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to members, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Extranet Website

Data Quality Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
0.1	First draft		January 2019	Kelly Huckvale Information Governance Officer Arden & GEM CSU

DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

RELATED DOCUMENTS:

Information Governance Management Framework

Information Governance Strategy

Confidentiality Code of Conduct

Information Security Policy

Data Protection and Confidentiality Policy

Access Control Policy

Safe Haven Policy

Email Policy

Internet Usage Policy

Risk Management Policy

Contents

1.	Introduction and Aims	4
2.	Scope.....	4
3.	Definitions	5
4.	Responsibilities	5
5.	Development Process NHS Number.....	6
6.	Validation	6
7.	Validation Methods	6
8.	Data Standards	6
9.	Training.....	7
10.	Monitoring.....	7
11.	Equality Impact Assessment Statement.....	7
12.	References and Associated Documents	7

1. Introduction and Aims

Lincolnshire West CCG ('the CCG') recognises that decision making at every level within the NHS whether financial, clinical or managerial needs to be based on information which is of the highest quality and accuracy.

Information is derived from individual data items which are collected from a number of sources either on paper, or more increasingly with the advent of the electronic patient record and electronic health records on electronic systems.

Data quality is crucial and the availability of complete, accurate, relevant, accessible and timely data is important in supporting patient care, clinical governance, management and service agreements for healthcare planning and accountability. A data quality policy and regular monitoring of data standards are a requirement of the NHS Digital Data Security and Protection toolkit and will enable the CCG to embed good Information Governance practice within the organisation.

The policy is one of the key policies supporting the overarching Information Governance Strategy and works in conjunction with other relevant legislation and policies:

- Data Protection Act 2018
- EU General Data Protection Regulations 2016
- Information Management and Lifecycle Policy
- Data Protection and Confidentiality Policy
- Information Governance Policy
- Information Security Policy
- Safe Haven Policy

This policy sets out:

- The standards required for data quality
- The importance of using the NHS number as the unique patient identifier
- How data quality is validated
- The importance of data standards
- Audits

2. Scope

This Policy applies to all Lincolnshire West CCG staff, including, permanent and temporary staff, secondees, contracted staff, students/trainees/apprentices voluntary workers.

In addition, this Policy applies to all third parties and others authorised to undertake work for and on behalf of the CCG.

3. Definitions

Data should be:

- Complete (in terms of being captured in full)
- Accurate (the proximity of the figures to the exact or true values)
- Relevant (the degree to which the data meets current and the potential user's needs) Accessible (data must be retrievable in order to be used and in order to assess quality) Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised standards – either national or local)
- Defined (understood by all staff who need to know and reflected in procedural documents) Appropriately sought (in terms of being collected or checked once during an episode) Appropriately recorded (in either paper or electronic format)

The General Data Protection Regulations 7 Principles have Data Quality as the core items for organisations maintaining their GDPR compliance

These principles are as follows:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data Minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

4. Responsibilities

Overall responsibility for information governance sits with the Senior Information Risk Owner who is the Head of Performance & Delivery, Information Governance and Information Managers are responsible for ensuring staff members have received the relevant training that is conducive to achieving data quality.

Data quality is a key part of any information system which exists within the organisation's structure. All staff members will be in contact with a form of information system, whether paper or electronic based and are obligated to maintain records accurately and legally (Data Protection Legislation), contractually (contract of employment) and ethically (professional code of conduct).

5. Development Process NHS Number

The NHS number is a unique patient identifier and must be recorded correctly and in all systems where patient information is present. The NHS number is required to be used in all referral forms and letters in accordance with NHS requirements and compliance with the revision in the H&SCA 2015 requirement on the consistent use of the NHS Number as the unique identifier for Health care data.

6. 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 to continuously and can also be used on historical data to improve quality.

Regular validation processes are undertaken by the Business Intelligence Team and Informatics Services on data processed in order to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include checking for duplicate data, ensuring that national definitions and coding standards are adopted and the NHS number is used and validated. Additional checks will be undertaken on Continuing Healthcare data to assess accessibility and timeliness.

7. Validation Methods

Validation should be accomplished using either of the following methods:

- Bulk reporting, which involves a large process of data analysis to identify all areas where quality issues exist and correct them.
- Regular spot checks, which involves data analysis on a random selection of records against source material if available. The number of records examined and the frequency of those checks should be agreed by the CCG
- Bulk reporting can be used as an initial data quality tool as this will quickly highlight any areas of concern. However, further investigation will be required to identify more specific issues. Spot checks should be done on an ongoing regular basis to ensure the continuation of data quality.

8. Data Standards

The use of data standards within systems can greatly improve data quality. These can be incorporated into systems either using electronic selection lists within computer systems or manually generated lists for services that do not yet have computer facilities.

Either method requires the list to be generated from National or locally agreed definitions and must be controlled, maintained and updated in accordance with any variations that occur. Any documentation that refers to the data standards must also be updated as needed and disseminated to all relevant parties.

9. Training

All staff must complete Data Security Awareness Level 1 training on an annual basis. The module can be completed via the Electronic Staff Record (ESR) training module.

Line Managers are responsible for identifying the training requirements of their staff and working with training providers to ensure these needs are met. Staff must be enabled to attend the appropriate training where it is identified.

10. Monitoring

Data quality is subject to internal control processes within the CCG. All information systems will have processes developed to systematically identify errors and other aspects of poor data quality.

Departments should undertake an internal audit of their records annually to ensure compliance as part of the internal control processing statement.

11. Equality Impact Assessment Statement

Arden and GEM aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with Arden and GEM's Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief.

The equality impact assessment has been completed and has identified impact or potential impact as 'no impact'.

Arden and GEM will endeavour to make sure this policy supports its diverse workforce look after the information the organisation needs to conduct its business. It will also endeavour to make sure that this information is protected on behalf of patients regardless of race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

12. References and Associated Documents

The following Information Governance policies are related and should be read in conjunction with this policy:

Data Protection and Confidentiality Policy
Risk Management Policy

Other Relevant Documentation:

Information Asset Management Procedure
Data Protection Act 2018
EU General Data Protection Regulations 2016

Lincolnshire West CCG policies and procedures are available to staff via the Intranet and are uploaded to the CCGs public facing website.

Staff will be made aware of new policies and procedures updates as they occur.