NHS
Bury
Clinical Commissioning Group

Data Quality Procedure

Version:	2.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Date ratified:	28 May 2021
Name of originator /author (s):	Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	June 2021
Review date:	
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Data Quality Procedure CCG.GOV.038.2.0
Category of Document in The Policy Schedule	Governance
Author(s) **Contact(s) for further information about this document**	Information Governance Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff.
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre, 1 Knowsley Place, Knowsley Street, Bury, BL9 0SN Phone 0161 253 7849
Copies of this document are available from	CCG Corporate Office CCG Website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = Policy first draft	Information Governance Team	10th January 2019
1.0 = Policy once ratified	Information Governance Operational Group	TBC
1.1= Policy once reviewed	IG Team	24th May 2021
2.0 = Policy once ratified	Information Governance Steering Group	28th May 2021

Data Quality Procedure

Table of Contents

1.0 Introduction

1.1 The purpose of this procedure is to ensure that Bury CCG (thereafter referred to as the CCG) process good quality data and have clear guidance in place to assist staff on how to achieve this.

1.2 The CCG recognises that decision making at every level within the NHS whether this is financial, clinical or managerial needs to be based on information which is of the highest quality and integrity. The information used in the CCG is derived from a multiple range of sources either on paper or electronically and the CCG must ensure that they have the assurance that information they produce or use from another source is of the highest quality.

1.3 Data Quality is crucial, and the availability and integrity of complete, accurate, relevant, accessible and timely data is important in supporting the aims of the CCG such as supporting patient care, managing staff, performance monitoring and management and planning of healthcare services. It also portrays accountability which is a one of the fundamental principles of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and is also reflected in the National Data Guardian Data Security standards.

1.4 Careful monitoring and error correction can support good quality data, but it is more effective and efficient for data to be processed correctly the first time. In order to achieve this, procedures such as this must exist so that staff are aware of the importance of Data Quality.

1.5 Where staff process data they need to ensure that this is of the highest quality it can be by ensuring it is accurate, up to date and that validity checks are made to ensure it remains as such. This is especially important when personal data, special categories of data and business sensitive data is processed.

This procedure sets out guidance required for achieving high Data Quality, the importance of using the NHS Number as the unique patient identifier (where appropriate within the CCG), data validation methods and the importance of data standards. It also supports the Data Security, Protection and Confidentiality Policy and works in conjunction with the other data security / information governance policies and procedures that are already in place.

1.7 This procedure supports the CCG to comply with the following Acts

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000

2. Scope

2.1 This procedure applies to

- those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility;
- staff covered by a letter of authority / honorary contract or work experience the organisations policies and procedures are also applicable whilst undertaking duties for or on behalf of the CCG; and
- all third parties and others authorised to undertake work on behalf of the CCG.

2.2 This procedure outlines good practice and identified the roles and responsibilities of the CCG and its staff in terms of Data Quality.

3.0 Definitions

3.1 The following definitions apply in respect to this policy:

- **Personal Data**

3.2 This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

- **Special Category Data**

3.3 This is personal data consisting of information regarding: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

3.4 For more information about special categories of data please refer to the ICO guide at: **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

- **Personal Confidential Data**

3.5 This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

- **Processing**

3.6 This means any operation or set of operations which is performed on personal data or on 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.

4. Data Quality Principles

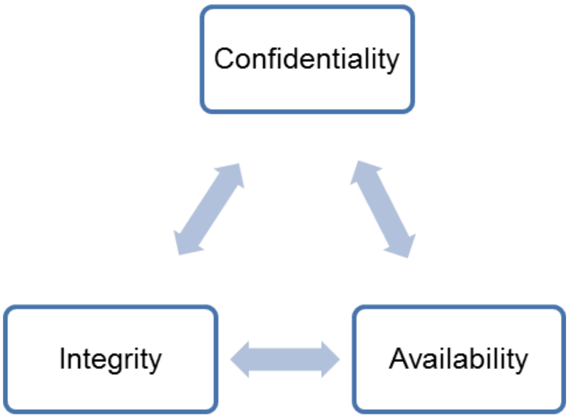
4.1 Personal and special category data is processed within the CCG by services who provide a direct care function for patients and by the commissioned Human Resources function as regards staff data.

4.2 Having accurate, relevant data that is accessible at the appropriate times is essential to each health management and / or business decision in order to deliver the aims and objectives of the CCG. All employees of the CCG must recognise the importance of Data Quality and their responsibilities in this area.

4.3 For the CCG, the importance of quality data is essential for:

- Patient care – delivery of effective, relevant and timely care and efficient administration (communication with patients and / or their representatives) (Continuing Healthcare / Medicines Management / Safeguarding);
- Staff management – delivery of an effective and efficient Human Resource, training and support service;
- Management and strategic planning – accurate data regarding the volume and type of patient activity required to provide appropriate allocation of resources and planning for future service delivery;
- Being able to undertake local and national benchmarking; and
- Compliance with GDPR, DPA 2018 and the National Data Guardian Data Security standards

4.4 Data Quality is a fundamental aspect of the (Confidentiality, Integrity and Availability (CIA) triad. This commonly used framework sets out the 3 main goals to achieve data security of which Data Quality is fundamental in order to achieve this.



4.5 **Confidentiality** is about privacy and ensuring information is kept confidential and only available to those with a proven need to see it.

4.6 **Integrity** is about information stored in, for example, a database being consistent, accurate and unmodified. Systems must be designed so that the input and management of information is not prone to human error (where possible) and that the flow of information does not result in loss or alteration. It is important to ensure that when data input is being carried out, the data items being processed is accurate and up to date. This applies also to manual processes such as printing address labels / writing addresses on an envelope, for example, information must be checked to ensure it is correct and up to date, so this is not inadvertently disclosed to someone else. Therefore, local departmental data validation checks are crucial to check the right information is being used at the right time. It is also important to remind patients (and their representatives) and staff to check that the information the CCG holds about them is correct. Therefore, regular data validation / checking exercises must be carried out to ensure the right information is recorded. Appendix 1 provides some questions for staff to use to ensure data is right.

4.7 **Availability** is about information being there when needed. System designs must include appropriate access controls and checks so that the information in the system has consistency and accuracy, it can be trusted as correct and can be relied on when providing services within the CCG. It is important therefore that data is accurate so this can be retrieved easily when needed again. For example, if something is input incorrectly such as the spelling of a surname then this may make the record non retrievable when required later or may be missed from reports thus providing an incorrect outcome. It is important to use a unique identifier / key to help with such issues such as the NHS Number for clinical systems.

4.8 The standards for good quality data are highlighted below:

- COMPLETE – in terms of being captured in full, have you got everything you need but do not be excessive
- ACCURATE – is the data right
- RELEVANT – does the data being processed meet current needs – do not be excessive – remember the GDPR principles
- ACCESSIBLE – data must be easily retrievable in order to be used as and when required and in order to assess the quality of it
- TIMELY – is the information recorded and available as soon after the event as possible so no information is missed or forgotten about
- VALID – is the data in an agreed format which conforms to recognised standards – either national or locally agreed
- DEFINED – can the data be understood by all staff who need to use it and also can it be understood by patients / staff if they have access to it or can this be easily explained to them
- APPROPRIATELY SOUGHT / COLLATED – is the data checked and collated correctly with the source and is it continually monitored to ensure the information remains accurate and up to date
- APPROPRIATELY RECORDED – is the data recorded accurately on either electronic systems / paper systems – are the checks in place to make sure this is the case

4.9 Where applicable within the CCG, 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 to NHS standards e.g. drop-down menus which allow only certain datasets to be selected and in some cases will not allow a user to move on until a dataset has been selected to ensure there are no gaps. Such lists must be controlled, maintained and updated in accordance with any changes that may occur locally or nationally. In addition, electronic validation programmes must not be switched off or overridden by operational staff.

5. Roles and Responsibilities

5.1 The Following roles and responsibilities apply in respect to this policy:

- **Accountable Officer**

5.2 The Chief Officer has overall responsibility for Data Quality ensuring that the CCG process data with all legal, statutory and good practice guidance to ensure it is of high quality.

- **Data Protection Officer (DPO)**

5.3 The DPO is responsible for developing, providing guidance and maintaining comprehensive and appropriate documentation that demonstrates commitments to and ownership of data security responsibilities under GDPR and the National Data Guardian Data Security standards including Data Quality standards. The role is supported by the Information Governance Team.

- **Caldicott Guardian**

5.4 The Caldicott Guardian has responsibility for ensuring that the CCG adhere to the Caldicott Principles and the National Data Guardian standards which underpin the need for high quality data for effective and efficient patient care. The role is supported by the Information Governance Team.

- **Senior Information Risk Owner (SIRO)**

5.5 The SIRO, with support of the Information Asset Owners, CCG Executive Directors / Heads of Service / Line Managers has responsibility for ensuring that all staff are aware of information risks and by ensuring information is of high quality mitigates risks revolving around data errors. The role is supported by the Information Governance Team.

- **Managers / Heads of Department / Information Asset Owners**

5.6 All managers are responsible for ensuring that staff are aware of and understand this procedure and the importance of Data Quality. Where required, line managers must ensure that systems are in place to validate / check the completeness, accuracy, relevance and timeliness of data processed by their teams.

- **Information Governance Operational Group**

5.7 The Information Governance Operational Group will be responsible for ensuring that the Data Quality Procedures are implemented throughout the CCG. This procedure will be reviewed and approved by this Group.

- **All staff**

5.8 All staff, including temporary and agency staff, are responsible for:

- Implementing and maintaining Data Quality and are obliged to maintain accurate information by law (GDPR / Data Protection Act 2018), contractually (contract of employment and Confidentiality Code of Conduct) and ethically (professional codes of practice);
- Compliance with relevant process document to maintain good Data Quality;
- Co-operating with the development and implementation of policies and procedures as part of their normal duties;
- Identifying the need for a change in policy or procedure as a result of becoming aware of a change to improve Data Quality resulting from national and / or local issues / initiatives; and
- Identifying training needs in respect of improving Data Quality and attending required training / awareness sessions to maintain / improve Data Quality

5.9 Failure to follow the requirements as set out in the policy may lead to disciplinary action

6. Key Legislation

6.1 Several acts and guidance dictate the need for good Data Quality which include (but are not restricted to):

- **UK General Data Protection Regulation 2021 (UK GDPR) / Data Protection Act 2018**
- **Privacy and Electronic Communications Regulation (PECR) 2003**

6.2 The EU General Data Protection Regulation (GDPR) was approved in 2016 and became directly applicable as law in the UK from 25th May 2018. The UK left the EU on 31 January 2020 and entered a transition period, which ended on 31 December 2020. Consequently, from 1 January 2021, UK GDPR now applies. This mirrors the EU GDPR and this is in harmony with the Data Protection Act (DPA) 2018.

6.3 The aim of GDPR is to protect the fundamental rights and freedoms of natural persons about the processing of personal data and the rules enabling the free movement of Personal Data.

6.4 All staff must adhere to the principles of the GDPR when processing personal and / or special categories of data and demonstrate compliance with these.

6.5 Article 5 of GDPR sets out seven key principles which lie at the heart of the data protection regime, this includes ensuring the secure transfer of information. It states that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

6.6 The seventh principle relates to “accountability” which makes the CCG responsible for complying with the GDPR and says that the CCG must be able to demonstrate compliance.

6.7 For further information relating to the accountability principle please see: **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/**

- **National Data Guardian Data Security Standards**

6.8 The National Data Guardian (NDG) Data Security Standards have been developed as a result of the National Data Guardian Review of Data Security, Consent and Opt-outs. These outline measures to ensure information at rest and in transit is secure. There are 10 standards which are clustered under 3 leadership obligations to address people, process and technology issues as follows: .

Leadership Obligation 1: People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: ensure technology is secure and up to date.

Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

- **The Caldicott Principles**

6.9 Before using or sharing confidential information, you must also consider the Caldicott Principles:

Principle 1: Do you have a justified purpose for using this confidential information? The purpose for using confidential information should be justified, which means making sure there is a valid reason for using it to carry out that particular purpose.

Principle 2: Are you using it because it is necessary to do so? The use of confidential information must be necessary to carry out the stated purpose.

Principle 3: Are you using the minimum amount of information required? If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose. Do not collate information just because it might be useful this is excessive and in breach of this principle.

Principle 4: Are you allowing access to this information on a strict need-to-know basis only? Before confidential information is accessed or transferred, a quick assessment should be made to determine whether it is needed for the stated purpose. If the intention is to share the information, it should only be shared with those who need it to carry out their role.

Principle 5: Do you understand your responsibility and duty to individuals with regards to keeping their information secure and confidential? Are you up to date with your training? Do you understand your responsibility for protecting information?

Principle 6: Do you understand the law and are you complying with the law before handling the confidential information? If not ask!

Principle 7: Do you understand that the duty to share information can be as important as the duty to protect confidentiality. However, it's important to remember if you are sharing this is done lawfully and securely.

- **Health and Social Care (Safety and Quality) Act 2015**

6.10 This promote the best practice standards to ensure a better cooperation and **protection of the public.**

- **Privacy and Electronic Communications Regulation (PECR) 2003**

6.11 PECR gives individuals privacy rights in relation to marketing, cookies and secure network communication services. The regulators recently banned cold calling initiatives by pension / claims operators as a consequence of violating consent guidelines in harmony with GDPR consent principle. PECR continues to apply alongside UK GDPR.

7. Data Standards

7.1 National NHS data standards exist to support the sharing, exchange and comparison of data across the NHS.

7.2 In certain situations, there may be no NHS national standards, for example, in a local database / system used to record Continuing Healthcare applications or to maintain a staffing database. In such cases, the CCG will agree local standards to be used. It is important that such local processes are regularly reviewed to ensure their continued validity and relevance.

7.3 In most cases however, the providers of services which the CCG commission use such standards such as acute trusts and mental health providers to accurately record activity but it is important to note the CCG then use and rely on this data (in an anonymised / pseudonymised form) to analyse and measure performance and manage service provision. In some cases, they may also be useful to apply to local CCG systems where patient data is being processed. The CCG therefore needs to be able to rely on the quality of the information being provided to it and this can be managed via adopting data standards such as below.

7 NHS Data Model and Dictionary Service

7.2 This provides common definitions, known as data standards, which are used in commissioning and make up the base currency of the Commissioning Data Sets (CDS). They are presented as a logical data model, ensuring that all standards are consistent and integrated across all NHS business areas. For the CCG on the monitoring side, they support accurate comparative data analysis, preparation of performance tables and mandatory data returns.

8 Information Standards Notices (ISN's)

7.3 These are used to define the who, how, what, when and where information can and should be collected and defines how data is passed between systems, users and processes ensuring the same message is sent and received. Changes to data standards and deadlines to adhere to such changes are made through ISN's. These changes must be monitored by the Information Asset Owners (IAO's) / System Administrators, to ensure compliance. IAO's must ensure that CCG information systems are updated in accordance with new ISN's to ensure system conformation. From a CCG and 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.

9 Clinical Coding

7.4 Although clinical coding is not directly applicable for a CCG, it is important to be aware of this and understand how this coded information is used by the CCG. Read codes are a coded thesaurus of clinical terms which are the basic means by which clinicians record patient findings and procedures in healthcare IT systems across primary and secondary care. The CCG works with GP's and secondary care to promote and improve Data Quality standards by assessing the quality of their clinical data and identify any problems ensuring that high quality data is maintained. For more information on this, please contact the Data Quality Team.

8. Data Validation Checks

10 Importance of data validation / checks

8.1 Validation and / or Data Quality checks encompass the processes that are required to ensure that data being processed is of good quality, accurate and reliable. It is imperative that regular validation processes and data checks / audits are undertaken on data being processed to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include checking for duplicate or missing data and ensuring that where required national and local standards are implemented and maintained.

11 Validation / data checking methods

8.2 Validation / Data Quality checking must be carried out using some or all the following:

- Wherever possible, computer systems will be programmed to only accept valid entries:
    - At data input – data accuracy is the direct responsibility of the person inputting the data supported by the line manager. Staff need to check the acceptability of the data from the direct source (e.g. patient / staff and / or their representative) or from the third party (e.g. provider data). Please see Appendix 1 for further guidance on this. Dependent upon the system, later validation may be necessary to maintain referential integrity. This refers to ensuring that when one database / system is linked to another the accuracy and consistency of data within that relationship is maintained.
    - Internal Validation – where applicable, systems incorporate internal validation processes and audit trails to detect and record any problems with processing / data integrity. For example, a system will not allow a user to type free text in a defined field which asks for certain items to be added
- Regular spot checks / audits – this involves analysis of a random selection of records such as staff personnel files or Continuing Healthcare files for patients against source material (if available). Spot checks must be undertaken on an ongoing regular basis to ensure Data Quality is not compromised and that information is up to date.
- Data Cross Checking – Making sure that data you have about a patient or staff member on one system and that which is held on another system are not disparate and if they are, then ensuring the correct information is held in both or more. What checks are done to ensure the right information is held?
- Templates – use of these allows data to be input in a consistent and coherent manner. It ensures that users enter all the required information about a patient or staff member which prompts the user to enter the key information required ensuring that accurate data capture occurs in order to carry out a required process such as a patient funding review or a staff application form for a training course. In addition, the CCG assists GP's in developing and reviewing templates to ensure consistency in the local area and to ensure performance reports are accurate.
- Source data – 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. Please see Appendix 1 for guidance.

- External sources of data – Where possible, validation processes should use the accredited external sources of information, for example, using the Patient Demographic Service (PDS) to check NHS numbers / death status. The CCG will use such sources to improve Data Quality.

8.3 Where data is shared between systems within the CCG and with the local authority, it is imperative that the source data be validated initially. Any modifications made to this data must then be replicated in other systems ensuring there are no inconsistencies. It is important to have synchronisation to ensure that all data sources reflect the same information.

9. NHS Number

9.1 The Health and Social Care (Safety and Quality) Act 2015 strengthened the requirement for health and adult social care organisations to use a consistent identifier (the NHS Number) for all data sharing associated with or facilitating care for an individual. A consistent identifier ensures that patients are identified consistently which is crucial to Data Quality and allows data linkage within and between different datasets.

9.2 Therefore, the NHS number must be used as the default unique patient identifier and systems used by the CCG providing direct care, this will mainly apply to the Continuing Healthcare, Medicines Management Teams and potentially the Safeguarding Team. Data Quality checks are undertaken to ensure the NHS Number is being utilised within systems / processes and within all associated correspondence such as letters to patients and / or their representatives. Validation checks are required to ensure that the right NHS Number is recorded for patients – this may require access to the Personal Demographics Service provided by NHS Digital.

10. Individual Rights

10.1 GDPR provides and strengthens the following rights for individuals regarding their personal data:

- The right to be informed (Article 12, 13 & 14)
- The right of access (Article 15)
- The right to rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 22)
- The right to withdraw consent (Article 7)
- The right to complain (Article 77)

10.2 As per the list above, two of the rights listed directly relate to Data Quality and accuracy of data which are the right to rectification and the right to restrict processing. The right to rectification states that patients / staff can request to have their data rectified if they believe this is inaccurate and the right to restriction states that an individual can also restrict processing if it is felt that data is inaccurate or not reliable. Staff must be aware of these rights and how to process them if in receipt of such a request. Therefore, it is important to ensure Data Quality checks are continually made to ensure the right information is available at the right time in order to prevent such rights being invoked. Further information about these rights can be in the Information Rights Procedure on CCG website.

11. Reporting Incidents and Monitoring Compliance

11.1 The CCG will monitor performance regarding the collation and processing of data to maintain good Data Quality standards in accordance to defined standards and provide appropriate feedback to staff, when necessary, to improve practices. The CCG are audited to check that the applicable legislation is complied with as named in this procedure and that suitable process and controls are implemented and maintained to ensure the completeness, relevance, correctness and security of data.

11.2 Each department is responsible for monitoring and maintaining the quality of the data processes and look to improve standards as and when required to mitigate data security incidents. Where a data security incident occurs linked to data quality, these are logged on the Data Security Breaches / IG Incidents Logbook and action plans are implemented to mitigate such events occurring in the future. Please remember to report any incidents / breaches regarding Data Quality following the CCG's incident reporting procedure or contact the Information Governance Team if you have any concerns / queries.

12. Training

12.1 When implementing a new system or a new process staff must be trained to ensure the information input into a system or used as part of a process is of the highest quality it can be. Effective and timely training will minimise the risk of data security incidents, input / typing / written errors, mistakes, reduce stress and increase the performance of staff.

12.2 Training allows staff to utilise new tools and potentially identify areas for improvement in Data Quality practices using new skills and techniques.

12.3 System / process specific training will help to:

- minimise confusion and mistakes when using a system / process
- improve data quality
- ensure that staff can take full advantage of new features that may improve Data Quality such as input validation on a system
- minimise unnecessary work for other staff solving minor problems
- make staff feel valued and empowered by updating their skills

12.4 It is the responsibility of Information Asset Owners / System Administrators to ensure that no access is granted on any system / process before relevant training has been completed. Ongoing support should be provided and a regular check on the competency of staff should also take place is deemed necessary by the Information Asset Owners / System Administrator.

13. Review

13.1 This procedure will be reviewed every two years, and in accordance with the following as and when required:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to CCG structure

14. Legislation and Related Documents

14.1 This procedure is available on the CCG's website and through the corporate folders.

14.2 Several other policies are related to this policy and all employees should be aware of the full range below:

- Data Security, Protection & Confidentiality Policy
- Records Management Policy
- Information Security Policy
- Acceptable Use of IT Policy
- Information Risk Policy
- Data Security & Protection Breaches / Incident Reporting Procedure
- Confidentiality Audit Procedure
- Confidentiality Code of Conduct
- Secure Transfers of Data Procedure
- Individual Rights Procedure

14.3 The CCG will also take action to comply with any new legislation / guidance relating to Data Quality.

15. Links and Further Information

- Data Protection Act 2018
  https://www.gov.uk/government/collections/data-protection-act-2018
- General Data Protection Regulation 2016 (GDPR)
  http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Health and Social Care (Quality and Safety) Act 2015
  http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- IG Alliance (IGA)
  https://digital.nhs.uk/data-and-information/looking-after-information/datasecurity-and-information-governance/information-governance-alliance-iga
- Records Management Code of Practice for Health & Social Care 2016

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

- Information Commissioners Office (ICO)
  https://ico.org.uk/
- The NHS Care Record Guarantee
- Caldicott 2 - Information: To Share or Not to Share? The Information Governance Review. London: Independent Information Governance Oversight Panel, 2013
- Caldicott 3 - Review of Data Security, Consent and Opt-Outs. : National Data Guardian, 2016
- Data Security and Protection Toolkit (DSPT) **https://www.dsptoolkit.nhs.uk/**

Appendix 1 - Data Quality Checklist

Below are some Data Quality questions to ask when processing personal and / or special categories of data to help you check that the data you are using is as accurate as it can be.

Information from the source

When undertaking Data Quality checks direct from the source (patient / staff member) ensure that you:

- Check that all the demographic details are correct – name, address, postcode, date of birth, NHS Number
- Check any other relevant information that you need for your purpose – for example, details of any representative and their contact details. Remember do not collate anything that is excessive as this could be a breach of the GDPR principles
- Record information accurately and as soon as possible so important information is not forgotten about
- Ask the source to check what you have documented to double check it is correct
- Undertake regular reviews of demographic data with the source to ensure the right data is recorded about them

When sending information

- Have you got the right contact details? Check them thoroughly and maybe ask others if they are aware of the recipient to check that you have the correct details
- If emailing – have you got the right email address – this is a common error and information can easily be disclosed to others inadvertently. If you are unsure, always check!
- If you need to send a blind copy email to everyone about something, ensure you do send it “BCC” – always check which address line you put batches of email addresses so you do not disclose to others
- Does a recipient wish to be contacted directly or does the communication need to be sent to their representative and in what format?
- How do you check that the contact details you have got are correct and up to date?

Information from third parties / external systems

- How is the information verified? Can you trust the information that is being supplied from a different source?
- Do you know how often the information is updated?
- What checks do you do to ensure the information is correct?
- Do you ensure other systems are updated if you become aware of updated / corrected information?