NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

Information and Data Quality Policy

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	76
Responsible Executive Director:	Deborah El-Sayed
Author and Job Title:	Alison Gane, SCW CSU Information Governance Consultant
Date Approved:	5 December 2023
Approved by:	Chief Executive Officer
Date of next review:	December 2024

Policy Review Checklist

	Yes/ No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Y	Included in the appendices
Has the review taken account of latest Guidance/Legislation?	Y	Key legislation mentioned reviewed by IG Consultant
Has legal advice been sought?	N	
Has HR been consulted?	Y	Via Corporate Policy Review Group
Have training issues been addressed?	N	Detailed in Policy document
Are there other HR related issues that need to be considered?	N	
Has the policy been reviewed by Staff Partnership Forum?	N	

	Yes/ No/NA	Supporting information
Are there financial issues and have they been addressed?	N	None identified
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	N	
Has the lead Executive Director approved the policy?	Y	Deborah El-Sayed, SIRO
Which Committees have assured the policy?		Corporate Policy Group and Information Governance Group
Has an implementation plan been provided?	Y	Included at the end of the policy.
How will the policy be shared with		Staff: the Hub, the Voice, Information Governance Group, Information Asset Owners and Asset Administrators
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	N	Not required
Has a DPIA been considered in regard to this policy?	N	Not required
Have Data Protection implications have been considered?	Y	Yes by IG Consultant

Version	Date	Consultation
1.0	March 2022	Corporate Policy Review Group

1.1	March 2023	Amendment to ICB template, update of Policy Introduction, Purpose, Scope, Definitions, Procedures and Controls. Addition of principles.
1.2	May 2023	Review and amendments requested by Corporate Policy Review Group and Data Protection Officer (DPO)
1.3	June 2023	Reviews by IGG and the addition of the Caldicott role added to Page 7

Table of Contents

Information and Data Quality Policy

Principles for Complete, Accurate, Relevant and Timely Information

1 Introduction

For proper decision-making, governance, and the continued delivery of high-quality healthcare, data quality is a necessity. The concept applies to the records, information and data that our organisation creates, maintains and utilises. The availability of accurate, quality and timely data is vital for the safe and responsible running of the ICB.

This policy outlines the standards anticipated in our systems, working practices, and processes to guarantee that high-quality information serves as the foundation for all of our organisation's functions. It aims to ensure that we create and perpetuate a culture of information quality throughout the ICB and with those that work in partnership with us to ensure reliable information is available to help the ICB achieve its goals. Any decision—clinical, managerial, or financial—must be supported by data that is of the highest quality and whose accuracy can be trusted by all users.

1.1 BNSSG ICB Values

This policy supports the ICB's data protection compliance which directly contributes the integrity of the ICB. Ensuring accurate and quality data is available to feed into decision making and ICB activities help us to strive for excellence.

2 Purpose and scope

This policy set out the ICBs statement of intent for ensuring it processes accurate, timely and complete data. It focuses on the principles that inform the relevant standard, ensures processes and procedures are implemented to ensure that data held and processed by the ICB is accurate, up to date and consistent. The Policy also details who is accountable for the requirements and the method for their measurement, reporting and delivery.

This policy is applicable to all records, information and data held and processed by the ICB. All information must be managed and held within a controlled environment and to a high standard of accuracy and completeness. This includes personal data of patients and staff, patient level data (non-identifiable – anonymised or pseudonymised) as well as corporate information. It applies to records, information and data regardless of format, in addition to legacy data held by the organisation, in accordance with the approved NHS retention standards.

3 Duties – legal framework for this policy

Quality is defined as information that is 'complete, accurate, relevant, available and timely'. The ICB in general will be in control of data and responsible for ensuring quality of data held and shared with others.

Key Legislative and Regulatory Environment:

- Health and Social Care Act 2012
- Public Records Act 1958
- UK General Data Protection Regulation /Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Common law duty of confidentiality
- Human Rights Act 1998
- Records Management Code of Practice for Health and Social Care 2020

The ICB recognises that effective information management is fundamental to good administration and operational effectiveness and is an enabler to achieve strategic values. High standards of information quality, supported by systematic processes and practice support high-quality healthcare and improve services to ensure that information is of good quality.

4 Responsibilities and Accountabilities

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner for the ICB is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at executive management level. The SIRO must provide the Chief Executive with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. This includes risk associated with data quality for example holding and using out of date or inaccurate data. The SIRO will commission an annual Internal Audit of the Data Security and Protection Toolkit (DSPT) which include data quality requirements. The SIRO is also responsible for ensuring the right resources in place to fulfil information governance requirements placed on the ICB.

Caldicott Guardian (CG)
The Caldicott Guardian has a responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian has an advisory role and a particular focus on ensuring patient identifiable information is processed in line with the Caldicott principles.

Data Protection Officer (DPO)
The Data Protection Officer (DPO) is the person identified within the ICB that has the responsibilities as set out in the UK GDPR guidance, this includes a role that will ensure that information governance incidents which are likely to result in a risk to the rights and freedoms of individual that the Information Commissioner Officer (ICO is informed within 72 hours, this includes and incidents arising from data and information quality concerns.

SCW Information Governance Lead
The SCW Information Governance (IG) lead supports the ICB with all areas of Information Governance. They manage the Information Governance programme and ensure implementation throughout the ICB. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit. The Information Governance Team will support the organisation in investigating Serious IG Incidents Requiring Investigation (SIRIs), offer advice and support for the organisation to comply with legislation, policies and protocols The IG Lead provide advice and guidance on data quality and related audits and incidents.

Information Governance Group (IGG)
The ICB Information Governance Group is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the ICB and raising awareness of Information Governance. Frequent audits by SCW IG lead will highlight what records have been accessed and the quality of the data that is being recorded.

Directors and line managers
Directors have overall responsibility for Data Quality policies, procedures, the implementation of controls and for making arrangements for staff to be aware of their responsibilities including through regular reminders and operational 'on the job' instruction. They also are responsible for responding to rectification requests and recording the outcome of any request. Line Managers are responsible for ensuring that staff are aware of and comply with policy requirements including through the provision of information as part of local induction.

Information Asset Owners/Administrators (IAO/IAA)
Each Directorate has one or more nominated Information Asset Owners (IAO) and Administrators (IAA). The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area and to promote data quality issues within the directorate, providing advice, supporting the completion of audits and sign posting to polices and guidance As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role.

All Staff
Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice. Data accuracy and security is

a contractual and legislative requirement, and a breach of this policy may result in disciplinary action.

5 Definitions/explanations of terms used

Processes
Means any operation or set of operations which is performed on personal data or on sets of personal data (whether by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction)

Anonymisation
Anonymisation means that individuals are not identifiable and cannot be re-identified by any means reasonably likely to be used (i.e., the risk of re-identification is sufficiently remote). Anonymous information is not personal data and data protection law does not apply.

You can consider data to be effectively anonymised when it does not relate to an identified or identifiable individual; or is rendered anonymous in such a way that individuals are not (or are no longer) identifiable.

Pseudonymisation
Pseudonymisation means that individuals are not identifiable from the dataset itself but can be identified by referring to other information held separately.
Pseudonymised data is therefore still personal data and data protection law applies.

Pseudonymisation is a technique that replaces or removes information that identifies an individual. For example, it may involve replacing names or other identifiers (which are easily attributed to individuals) with a reference number. This is similar to how the term 'de-identified' is used in other contexts, for example the removal or masking of direct identifiers within a dataset.

Personal Data
"Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as;

1. Names (i.e., Name, Surname)
2. Location - such as a home address, postcode, or mobile phone GPS
4. Telephone numbers
5. Online identifier, such as an IP or email address
6. Identification identifiers – such as National Insurance, NHS Number, Account Numbers, Photos, Vehicle Registration Plates.

Please note the list above is provided to give an indication as to what is classified as personal data and is not an exhaustive list of identifiers.

6 What is Data Quality?

Data quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever it is required. Data quality is vital to effective decision making at all levels of the organisation.

7 Data Quality Standards

Accessibility
Information can be accessed quickly and efficiently using systematic and consistent management in electronic and physical formats. Access must be appropriate so that only those with a lawful basis and legitimate relationship to information can view, create, or modify it.

Accuracy
Information is accurate and supported by appropriate systems, processes, guidance and practices. This is a legal requirement of the Data Protection Legislation that 'personal data shall be accurate, and where necessary, kept up to date'. Ideally, systems will capture data once and ensure that accuracy is maintained and checked through process.

Any limitations on accuracy of data must be made clear to its users and effective margins of error built into calculations.

Completeness
The relevant information required is identified. Systems, processes and working practices ensure it is routinely captured. The specification of what data is required for the defined need will be incorporated into processes, collection, and validation.

Evaluation of information quality must include checks for missing, incomplete or invalid information and consider the causes for this and any associated risks.

Relevance
Information is kept relevant to the issues rather than for convenience, with appropriate management and structure.

Reliability
Information must reflect a stable, systematic and consistent approach to collection, management and use. Methods of collection, use and analysis must ensure consistency in the data and variations in these methods must be considered for their potential impact on the quality or content of the information.

Timeliness
Information is recorded as close as possible to being gathered and can be accessed quickly and efficiently. This is a requirement of the Data Protection Legislation 'personal data shall be accurate, and where necessary, kept up-to-date'.

Validity
Information must be collected, recorded and used to the standard set by relevant requirements or controls. Validity is supported by consistency over time, systems and measures. Any information collection, use or analysis process should incorporate a proportionate validation method or tool to ensure that the standards and principles outlined above are met. Validation tools and processes will support routine data entry and analysis, as well as support the identification and control of duplicate records and errors.

Data Dictionary Change Notices/Information Standards Notices
Data Dictionary Change Notices (formerly Information Standard Notices and Data Set Change Notices) are issued by the Health and Social Care Information Centre. These give notification to NHS healthcare agencies of changes to information requirements that will be included as appropriate in the NHS Data Dictionary & Manual and thereby ensuring that data is meaningful across NHS Organisations over time. The SCW CSU Data Management Team will monitor the publication schema for DDCNs and ensure all DDCNs relevant to the ICB are sent for relevant action to the appropriate team.

NHS Number
The NHS Number is the unique identifier within the National Health Service. Where appropriate and legal to be used, it must be incorporated into all correspondence with patients and relevant information systems to ensure that the correct individual is identified.

Services that are commissioned are contracted to the use of an NHS Number, where appropriate, and to ensure it is incorporated into routine data collection, data management and working practice. Appropriate mitigation is required from commissioned services in clinical and commissioning systems for the absence of an NHS number for an individual.

8 Data Accuracy Procedures

The ICB is committed to ensuring that all information within its responsibility is created, processed and held to a high standard of quality in a manner which ensures accurate and appropriate decision making.

We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

i. Authentic – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed;
ii. Reliable – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records;

iii. Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified;
iv. Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

9 Controls

Rule based processing of information

This control generally applies to electronic systems and relates to any 'automated' process that takes inputted data and processes it into another form, such as creating a result from a calculation run on two data fields.

Elements of an information system that run an internal process on data will be specified in developments and tested before system acceptance. Checks will be run as part of change control and system acceptance procedures when system developments affect any of the internal processing.

Standard system reports or processes will be checked so that if they have a running order this is maintained.

Authenticating data (on systems, and in messages)

Data items in paper format will be subject to rules for ensuring identification of the author. Typically, reliance is on a dated signature of staff completing forms or records.

Data items in electronic format will be attributed to the User ID recorded in any audit trail relating to the creation, viewing, amendment or deletion of data.

Ongoing use of smartcards for electronic patient records and the electronic staff record will ensure a robust level of authenticity provided cards are used and managed appropriately, as per national and local smartcard policy and procedure.

Validation of information displayed or extracted

Despite implementation of controls on both data collection/input and internal system processing, data cannot be entirely relied on without further checks on output. For the purpose of this policy output is defined as follows:

Regular or ad-hoc reports compiled from summary of information on multiple records.

Information analysis staff will be responsible for running regular validation checks on reports. Confirmation of the validity will require input from the system owners. Typically reports can be validated by comparison with other data/reports.

Staff line managers will have a default responsibility to ensure their employees are familiar with processes/procedures around handling data output, especially with regard to interpretation.

Checking patient details (demographics validation)

Administrative processes will include checking the detail of patient records, such as name, address, date of birth, GP etc. with the patients themselves.

Patients (and others making enquiries) must be asked to confirm demographic details to staff, rather than staff informing them of the details (such as address) and asking if it is correct. This is to ensure that patient demographics are not disclosed inappropriately to third parties, and that patients can choose how to confirm details to staff, if they are perhaps unhappy about informing staff of details verbally in open public areas.

The ICB will ensure it have monitoring in place to identify and resolve duplicate records.

10 Requests for Rectification

In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Citizens have the right to the rectification of their information in the instance that their records are inaccurate or incomplete. These requests will be handled in line with the ICB policy.

11 Training requirements

All staff are required to complete annual Data Security Awareness training.

12 Equality Impact Assessment

Equality Impact Analysis (EIA) screening has been completed and a full assessment is not required. A copy of the EIA screening is attached at Appendix 15

13 Implementation and Monitoring Compliance and Effectiveness

The ICB will ensure that information governance is part of its annual cycle of internal audit. The results of audits will be reported to the ICB Information Governance Group along with relevant action plans which they will monitor.

Compliance with the ICB policies is stipulated in staff contracts of employment. If staff members are unable to follow the ICB policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with the ICB policies or failure to report non-compliance may be treated as a disciplinary offence.

14 Countering Fraud, Bribery and Corruption

The ICB is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document. In some case the matter may be referred to the Local Counter Fraud Specialist or, if severe the Police for further investigation.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the individual Team member will refer the matter to the ICB's Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts.

15 References, acknowledgements and associated documents

This policy should be read in conjunction with the following:

- Records Management Policy
- Confidentiality and Security of Information Policy
- Information Risk Management Policy
- Freedom of Information and Environmental Information Regulations Policy
- Individuals Rights Policy

15. Appendices

15.1 Equality Impact Assessment

Equality Impact Assessment Screening	
Query	**Response**
What is the aim of the document?	The Information and Data Quality Policy details how the ICB will meet its legal obligations and requirements concerning the management operational requirements of information and data quality.
Who is the target audience of the	All staff
document (which staff groups)?	

Who is it likely to impact on and how?	Staff	X
	Patients	X
	Visitors	X
	Carers	X
	Other – governors, volunteers etc	X
	Age (younger and older people)	No – the Policy applies to the quality of information and is applied equally
Does the document affect one group more or less favourably than another based on the 'protected characteristics' in the Equality Act	Disability (includes physical and sensory impairments, learning disabilities, mental health)	
	Gender (men or women)	
	Pregnancy and maternity	
	Race (includes ethnicity as well as gypsy travellers)	
	Sexual Orientation (lesbian, gay and bisexual people)	
	Transgender people	
	Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)	
	Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)	

15.2 Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	Awareness of Policy	Launch of Policy shared at HWGNFY	AG	July 2023	August 2023	Time on agenda
Staff	Access to policy	Upload on to Hub	RH	June 2023	June 2023	Comms support
Staff	Awareness of Policy Changes	Newsletter and upload to Hub	AG	June 2023	July 2023	Comms Support