University Hospitals Bristol NHS
NHS Foundation Trust

Data Quality

Document Data		
Subject:	Procedural Documents	
Document Type:	Policy	
Document Status:	Approved	
Document Owner:	Head of Information	
Executive Lead:	Director of Finance	
Approval Authority:	Risk Management Group	
Estimated Reading Time:	15 Minutes	
Review Cycle:	48	
Next Review Date:	**Date of First Issue:**	**Date Version Effective From:**
01/07/2017	13/03/2003	29/06/2015

Document Abstract
Data Quality is defined by information being complete, accurate, relevant available and timely. It is a requirement of the Data Protection Act that all data should be adequate, relevant and not excessive plus that it is accurate and up-to-date. Good quality data is also essential to protect patient safety and underpins performance monitoring and service monitoring. Therefore, it is essential that policies and procedures are in place that outline the ways that the Trust assures itself that its data collection and processing is done to the highest standard.

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions**	**Type of Revision**	**Description of Revision**
01/08/2013	4.00	Head of Information	Minor	First draft
20/06/2015	5.00	Head of Information	Minor	Changes to job titles and groups
20/08/2015	6.00	Clinical Audit & Effectiveness Manager	Minor	Clarification of Clinical auditing role in data quality checks

Table of Contents

1. Introduction

Safe and high quality patient care is underpinned by the collection of quality data, which will inform all aspects of the Trust's activity, for example, informing patients of upcoming appointments; assuring that the Trust delivers timely and effective treatment or care for the patient.
As a data controller under the Data Protection Act 1998, the Trust has a legal responsibility to keep data held accurate and up-to-date and must take all reasonable steps to ensure good data quality. Quality is defined as information that is 'complete, accurate, relevant, available and timely'.

2. Purpose and Scope

The purpose of this policy is to outline / define the steps that the Trust will take to ensure that it has procedures in place for the collection and recording of accurate, complete information and establish the requirements for training of staff in good data collection practices. These data collected may be for the direct care of patient, staff attendance / absence records, or any other data collection that supports Trust in its day to day activities.

Whilst a clinical negligence case itself may not be caused by poor quality information, any defence by the Trust can be compromised if information is of poor quality.

The scope of this policy is to cover all paper based or electronic data collection which is person-based and required as a formal record of the Trust.

3. Definitions

ASH – Accredited Safe Haven: authorised by the Health and Social Care Act to receive patient identifiable data.

SUS - Secondary Uses Service: The agency that manages the forward transmission of data to commissioners and Department of Health (DOH); the mechanism by which data are sent to the commissioners and the DOH about each patient episode.

ISN – Information Standards Notice; All NHS approved changes to the Data Model are published at http://www.hscic.gov.uk/hesdatadictionary

Medway Sigma – the Trust's patient administration system and electronic patient record.

InfoWeb – accessed via Connect (Trust Intranet) gives a series of reports to aid managers in accessing performance reporting and reporting to support service delivery and planning.

PHD – The Patient History Database, an archive of data from Medway and other clinical systems used for in house reporting.

ESR – Electronic Staff Record; the national database which stores all information related to employees / applicants.

NHS Spine Portal Smartcard – used to authenticate staff's access to IT systems whether national or local.

4. Duties, Roles and Responsibilities

4.1 Trust Board of Directors

(a) The Chief Executive is the Accounting Officer of the Trust and has overall accountability and responsibility for Information Governance, of which data quality is one element**.**

4.2 Executive Directors

(a) The Director of Finance and Information –executive lead for Data Quality, has overall responsibility for the quality of data.

(b) The Medical Director - the Senior Information Risk Owner (SIRO) owns all information risks for the Trust, including the information risks associated with poor data quality.

4.3 Trust Management Groups

(a) The Information Risk Management Group monitors data quality reports as required by the Information Governance Toolkit.

(b) Benchmarking and outliers as reviewed by the Trust's Quality Intelligence Group (QIG) chaired by the Medical Director (SIRO).

(c) The Clinical Record Keeping Group will review the outcomes of the annual heath records audit, coordinated through the Clinical Audit & Effectiveness Team and undertaken by clinical staff within Divisions. This audit will be conducted on paper-based records and electronic patient records within the Electronic Document Management system (EDM), supporting the Trust's Information Governance Agenda and the NHS Litigation Authority.

4.4 Divisional Management Boards

(a) Will monitor data quality via reports produced by the Information Analysts in conjunction with other Divisional staff. Be responsible for action on improvement plans produced to address areas of high risk in relation to data quality (e.g. the annual health records audit results).

4.5 Line Managers

(a) Line managers of staff will have default responsibility to ensure their staff are aware of processes and procedures relating to the quality of data.

4.6 All Staff

(a) Have the responsibility to collect quality information in line with policy and procedure.

5. Policy Statement and Provisions

5.1 Collection of information

Whether the system collecting information is paper based, e.g. clinical noting within a patient's case notes, or electronic, e.g. the recording of person demographics in an index such as the master patient index or ESR, then data collection processes will have rules-based data input designed into them either by having mandatory fields with drop down lists (within an IT system) or paper forms providing tick boxes or similar pre-defined options, so that only values within the determined range will be accepted.

Patient Identifier – In addition to the Trust number, the NHS Number will be used as the common identifier (across health and social care) on all patient records and correspondence. The Trust will develop processes and procedures to collect, transfer, capture and use the NHS number.

To prevent the incidence of missing or incomplete data on: -

(a) Paper based systems

Where possible, these systems will have printed forms providing tick boxes or similar pre-defined options and free text fields where no other option is available. Paper collection forms will indicate where the required collection is either numeric or character based and will indicate mandatory data items which must be completed.

(b) Electronic systems

Will ensure that data collection fields will only accept characters relevant to the data item being collected (e.g. numeric characters will not be allowed in 'name' fields). Electronic systems will feature rules that indicate to users when required data items have not been completed before data collection screens can be saved to the database.

Information Asset /System Managers (IAAs) will be involved in data input / collection data validation processes in order to ensure that the above guidelines are successfully applied.

Each system will have training guides that link to Standard Operating Procedures - a checklist of core processes for data collection. These will be reviewed periodically or as a need arises via feedback / quality monitoring and incidents. They will cover items such as registering and amending patient details, capture of referral / diagnosis, attendance and outcome data, removal of patients and caseload management.

Responsibility for review and development of input/collection validation will by default lie with the system manager. The Information Governance Officer will support Information Asset administrators/system managers in the application of these guidelines.

The Trust will nominate a senior member of staff to receive and implement 'Information Standards Notices' from the Health and Social Care Information Centre (HSCIC).

5.2 Rule based processing of information

This control generally applies to electronic systems and relates to any 'automated' process that takes input 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.

5.3 Authenticating data (on systems, and in messages)

The Clinical Record Keeping Policy sets the standard for signing and dating clinical notes.

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.

On-going 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.

5.4 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 the use of:

- Regular or ad-hoc reports compiled from aggregation of data, which may be run by users or Information Analysts.
- Viewing and use of individual records (both paper and electronic) for delivery and management of care.

Information analysts 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

Use of individual records (paper and electronic) within the delivery and management of care will be checked (NHSLA).

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.

5.5 Checking patient details (demographics)

All departments with direct contact with patients will ensure that their administrative processes include asking patients to confirm the detail of their records including spelling of name; address, date of birth, and GP practice. At a first appointment all details must be

checked to ensure that the correct record is selected or created. The majority of details should be checked at other appointments in order to pick up any changes or previous errors.

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 others (such as ex partners), and that patients can choose how to confirm details to staff. If patients express concern about being regularly asked to confirm their details they should be informed that standard checks are in place to ensure that mistakes are not made in relation to their care. Pre-registration forms can be used if patients are reluctant to give their details out loud in clinics.

6. Standards and Key Performance Indicators

6.1 Health and Social Care Information Centre (HSCIC)

Monthly Secondary Uses Service (SUS) data quality reports of submitted data items for Outpatient attendances, Inpatient admissions and discharges and Accident and Emergency attendances are produced to enable local and national benchmarking of Trust data quality on a number of different key performance indicators.

Other key performance are produced locally and monitored by Trust Executives, Divisional Boards and other key committees of the Trust.

7. References

7.1 NHS Data Model and Data Dictionary - specification of data items to be collected and commissioning data sets. The NHS Data Model and Dictionary provides a reference point for assured information standards to support health care activities within the NHS in England. It has been developed for everyone who is actively involved in the collection of data and the management of information in the NHS. http://www.datadictionary.nhs.uk/

7.2 Information and Performance reporting (Infoweb) – Trust information web pages that are designed to provide a central repository for information and performance reporting, which brings together sets of reports covering areas that are important to the Trust in its continuing drive for performance and service improvement. Infoweb includes Key Trust Performance Reports (including quality indicators).

7.3 Medway home page (http://medwayhome/Pages/MedwayHome2.aspx) provides resources and support for users including user guides, standard operating procedures and e-learning.

8. Appendix A – Monitoring Table for this Policy

8.1 Monitoring of this policy is managed via a number of audits, particularly those dictated by the Information Governance Toolkit, as below -

Monitoring activity	Detail	Description	Monitoring Group	Frequency	Who?
Information Governance Toolkit audits	Requirement 404	Multi-professional audit of clinical record keeping	Clinical Record Keeping Group	Annually	Clinical Governance team
Information Governance Toolkit audits	Requirements 502	Monitoring SUS Data Quality reports	Information Risk Management Group	Monthly	Information Team
Information Governance Toolkit audits	Requirement 504	Local and national benchmarking	Information Risk Management Group	Monthly	Information Team
Information Governance Toolkit audits	Requirement 505	Clinical coding audits	Information Risk Management Group	Internal – ad hoc External annually	Information Team
Information Governance Toolkit audits	Requirement 506	Accuracy check on service user data - audit	Information Risk Management Group	Annually	Information Team
Information Governance Toolkit audits	Requirement 507	Completeness and Validity Data audit check	Information Governance Management Group	Annually	Information Team

9. Appendix B – Dissemination, Implementation and Training Plan

9.1 The following table sets out the dissemination, implementation and training provisions associated with this Policy.

Plan Elements	Plan Details
The Dissemination Lead is:	Head of Information
This document replaces existing documentation:	Yes
Existing documentation will be replaced by:	Data Quality Policy
This document is to be disseminated to:	Trust-wide
Training is required:	No
The Training Lead is:	N/A

Additional Comments
[DITP - Additional Comments]

10. Appendix C – Document Checklist

10.1 The checklist set out in the following table confirms the status of 'diligence actions' required of the 'Document Owner' to meet the standards required of University Hospitals Bristol NHS Foundation Trust Procedural Documents. The 'Approval Authority' will refer to this checklist, and the Equality Impact Assessment, when considering the draft Procedural Document for approval. All criteria must be met.

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
Title	The title is clear and unambiguous:	Yes
	The document type is correct (i.e. Strategy, Policy, Protocol, Procedure, etc.):	Yes
Content	The document uses the approved template:	Yes
	The document contains data protected by any legislation (e.g. 'Personal Data' as defined in the Data Protection Act 2000):	Yes
	All terms used are explained in the 'Definitions' section:	Yes
	Acronyms are kept to the minimum possible:	Yes
	The 'target group' is clear and unambiguous:	Yes
	The 'purpose and scope' of the document is clear:	Yes
Document Owner	The 'Document Owner' is identified:	Yes
Consultation	Consultation with stakeholders (including Staff-side) can be evidenced where appropriate:	Yes
	The following were consulted: Trust Caldicott Guardian	Yes
	Suitable 'expert advice' has been sought where necessary:	Yes
Evidence Base	References are cited:	Yes
Trust Objectives	The document relates to the following Strategic or Corporate Objectives:	Yes
Equality	The appropriate 'Equality Impact Assessment' or 'Equality Impact Screen' has been conducted for this document:	Yes
Monitoring	Monitoring provisions are defined:	Yes
	There is an audit plan to assess compliance with the provisions set out in this procedural document:	Yes
	The frequency of reviews, and the next review date are appropriate for this procedural document:	Yes

Checklist Subject	Checklist Requirement	Document Owner's Confirmation
Approval	The correct 'Approval Authority' has been selected for this procedural document:	Yes

Additional Comments
[DCL - Additional Comments]