Information Quality Policy

WOOSEHILL MEDICAL CENTRE
JULY 20

Contents

1. Introduction

The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation. The effect of poor quality must be seen in a wider context of the potential impact it can have on patient care and there is potential that organisations could breach an individual's human rights where information that they use to treat a patient is of poor quality. This policy outlines our policy for ensuring data accuracy.

2. Legal requirements for quality information

The organisation is required to operate policy and processes to ensure that information is of good quality. Quality is defined as information that is 'complete, accurate, relevant, available and timely'. The Practice will in general be a Controller of personal data and responsible for ensuring quality of data held and shared with others.

General Data Protection Regulation 2016

The General Data Protection Regulation (GDPR) states that personal information should be "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'); (Article 5(1)(d)). Poor quality information will almost certainly breach this principle.

The Practice is required to take all reasonable steps to ensure the quality of its information.

Human Rights Act (1998)

Mistakes in a patient's record can lead to clinical errors in treatment, resulting in harm or even death of patients. Such instances are likely to be breaches of the Human Rights Act (1998), especially Article 2 (right to life) and Article 3 (protection from degrading treatment) and clearly lead to clinical negligence cases.

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

3. Responsibilities

The **Operations Manager** has overall responsibility for Data Quality policies and procedures and for staff training in data quality and for monitoring data quality throughout the organisation. They also are responsible for responding to rectification requests and recording the outcome of any request.

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 to the **Operations Manager.** Frequent audits will highlight what records have been accessed and the quality of the data that is being recorded.

Data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action.

4. Data Accuracy Procedures

We commit to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will "maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided";

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.

5. 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 and guidelines detailed in medical record policies and procedures 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. These may be run by users or specific Information Analysis staff
- View and use of individual records (both paper and electronic) for delivery and management of care

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.

Use of individual records (paper and electronic) within the delivery and management of care will be checked as part of a regular programme by clinical audit departments.

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)

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.

6. 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 Individual Rights Policy.]***

Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the IP rights of this document belong to SCW.

Document Name	Version	Status	Author
Information Quality Policy Primary Care template	1.0	Published	NHS SCW Information Governance Services
Document objectives:	This document supports Practice staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Monitoring arrangements and indicators:	This document will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Approved and ratified by:	**Woosehill Medical Centre**	Date: 28/07/2020	
Date issued:	28/07/2020		
Date uploaded to Website	25/09/2020		
Review date:	01 April 2021		

Change record

Date	Author	Version	Page	Reason for Change
21.07.2020	SCW	1	All	Review for Website publication