



MAYDEN Health
Policies and Procedures

IG05

Data Quality Policy

Information Governance

August 2010

IG Policy Index	
IG01	Information Governance
IG02	Information Security
IG03	Personal Information Handling
IG04	Confidentiality Code of Practice
IG05	Data Quality Policy
IG06	Risk Management
IG07	Security Incident Policy
IG08	Lifecycle Management
IG09	Business Continuity Plan

Current Version

Responsibility of	Information Governance Lead
Reviewed by	
First Issued	November 2009
Last Review Date	August 2010
Next Review Date	August 2011

Version History

Version	Date	Comment	Initials	Signature
1.0	3/12/09	Initial version following wide comment	CM	
1.1	23/8/10	Update to reflect latest position and practices	CM	

Roles and Responsibilities

Information Governance Lead	Chris May
Information Security Lead	Chris Eldridge

CONTENTS

1	Introduction	1
2	Scope.....	1
3	Definition of Data Quality	1
4	Core Principles	1
5	Importance of Data Quality	2
6	NHS Number	3
7	Validation of Data	3
7.1	Importance of Validation	3
7.2	Validation Methods.....	3
7.3	Data Standards.....	4
7.4	External Sources of Data.....	4
7.5	Source Data.....	4
7.6	Synchronising Information Systems.....	5
7.7	Timescales for Validation	5
8	Training and Communication.....	5
8.1	Training	5
8.2	Communication.....	5

1 Introduction

The Company recognises that all its decisions, whether clinical, managerial or financial; need to be based on information which is of the highest quality. All this information is derived from individual data items which are collected from a number of sources either on paper, or more increasingly, on electronic systems.

Data quality is crucial and the availability of complete, accurate and timely data is important in supporting ongoing patient care, integrated governance, management and service agreements for all of Mayden Health's strategic and planning and accountability.

2 Scope

This policy is intended to cover all data entered onto computerised or paper systems. It applies to all clinical and non-clinical data.

This policy is designed to ensure that the concept and importance of data quality to Mayden Health is disseminated to all staff. It will describe the meaning of data quality, who is responsible for its maintenance and how it can continue to improve in the future.

This policy applies to those members of staff who are directly employed by Mayden Health and for whom the Company has legal responsibility.

3 Definition of Data Quality

Data quality is a measure of the degree of usefulness of the data for a specific purpose. Data needs to be:

- Complete (in terms of having been 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 potential user's needs)
- Accessible (data must be retrievable in order to be used and in order to assess its quality)
- Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised national standards)
- Defined (understood by all staff who need to know and reflected in procedural documents)
- Appropriately sought (in terms of being collected or checked only once during an episode)
- Appropriately recorded (in both paper and electronic records)

4 Core Principles

As with other Companies, Mayden Health will be required by Connecting for Health to achieve certain levels for Data Quality as set out in the Information Governance Toolkit.

The Data Protection Act 1998 requires that information is accurate and up-to-date. <http://www.opsi.gov.uk>. It is vital to observe the 8 principles of the Data Protection Act 1998 – please see appendix 1.

Data quality is a key part of any information system that exists within the Company's structure. All staff members will be in contact at some time with some form of information system, whether paper or electronically based. As a result, all staff members are responsible for implementing and maintaining data quality and are obligated to maintain accurate records legally (Data Protection Act 1998), contractually (contract of employment) and ethically (professional code of practice).

There will be identified individuals within the Company with particular responsibility for data quality issues (eg, informatics, data protection, etc). Responsibilities concerning data quality will be explicitly stated in the job descriptions of staff involved in the collection or processing of data that is input to information systems.

Responsibility for the strategic management of data quality in the Company will lie with the Deputy Managing Director.

Responsibility for the operational management of data quality will lie with the Deputy Managing Director.

The importance of achieving good data quality will be addressed with all relevant staff as part of the induction process at commencement of their employment.

All data collection and input processes will have an audit trail and any training and development needs will be addressed.

All users will be made aware of their individual and the Company's corporate responsibility for confidentiality and security of data through the Company's relevant policies and training.

5 Importance of Data Quality

Quality information is essential for:

- Efficient administrative and clinical processes, such as communication with patients, their families and other carers involved in the patient's treatment.
- Management and strategic planning, requiring accurate data about the volume and type of previous patient activity and the population health needs to provide appropriate allocation of resources and future service delivery.
- Establishing acceptable service agreements for healthcare provision.
- Clinical governance, which depends on detailed, accurate patient data for the identification of areas where clinical care could be improved.
- Providing information for other Organisations – healthcare commissioners and providers depend on the patient data we send them and need to have confidence in its quality.
- Being able to benchmark Mayden Health's strategic and operational delivery against other similar organisations / companies.
- To facilitate and maintain the accurate flow of information between Mayden Health and external agencies.

6 NHS Number

An NHS number is the only unique way of identifying patients in an NHS system. With this in mind, it is imperative that this be recorded correctly and in all systems where patient information is present.

The NHS number is fundamental to the Connecting for Health National Programme for Information Technology (IT) as it is the common unique identifier that makes it possible to share patient information across the whole of the NHS safely, efficiently and accurately. The NHS number is the key to unlock services such as NHS Care Records Services (CRS), Choose and Book and the Electronic Prescription Service.

Every NHS patient is issued an NHS number either at birth (England and Wales) or when they join the NHS by registering with a GP practice. It is a unique 10 digit number where the first 9 are the identifiers and the tenth is a check digit used to confirm the number's validity.

It is the patient's unique NHS number that will allow the NHS staff to quickly and efficiently locate the correct health care records on the NHS CRS.

On 18/09/2008, the National Patient Safety Agency (NPSA) together with organisations in England and Wales recommended that they use the NHS Number as the national unique patient identifier.

<http://www.npsa.nhs.uk/corporate/news/nhsnumber/>

7 Validation of Data

7.1 Importance of 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 continuously and also can be used on historical data to improve its quality.

It is imperative that regular validation processes be undertaken on data being recorded to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include checking for duplicate data and ensuring that national definitions and standards are adopted and that the NHS number is used and validated.

7.2 Validation Methods

Validation should be accomplished using either of the following methods:

- Bulk reporting which involves a large single process of data analysis to identify all areas where quality issues exist and correct them.
- Regular spot checks which involve data analysis on a random selection of records against source material if available. The number of records examined and the frequency of these checks should be agreed within Mayden Health.
- 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 must be done on an ongoing regular basis to ensure the continuation of

data quality. Mayden Health will work towards developing a process for external audits to be undertaken annually in addition to the internal audits, where appropriate.

7.3 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 may occur. Any documentation that refers to the data standards must also be updated as needed and disseminated to all relevant parties.

Providers of data must also ensure that they are able to comply with data accreditation, health records accreditation when applicable and undertake routine data quality audit and quality monitoring.

Data quality is an essential part of the overall information governance (IG) framework and is a requirement of the IG toolkit for all data providers.

The legislative framework within which data standards should comply includes:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- National Health Services Act 1977

7.4 External Sources of Data

The validation process would use accredited external sources of information, for example, the National Strategic Tracing Service to check NHS numbers, etc.

Data pertaining to Secondary Uses Services (SUS), Payment by Results (PbR) and Commissioning coming from external providers and/or information services (including the Health Informatics Service [HIS] and Commissioning Business Support Agency [CBSA]) should have their own data quality policies which are required to meet national standards. The same is valid for third party data/information, eg, Social Services.

7.5 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.

7.6 Synchronising Information Systems

In situations where data is shared between systems it is imperative that the source data be validated initially. Any modifications made to this data must be shared with other related systems ensuring there are no inconsistencies between them. These systems must then be examined and authenticated in turn. Continuous synchronisation between systems is required to guarantee that all data sources reflect the same information.

7.7 Timescales for Validation

Where inconsistencies are identified these must be acted upon in a timely fashion and documented. Locally agreed deadlines will apply to the required corrections but all amendments should be made within a maximum of two months from the identification date.

Note: Under the Data Protection Act 1998 (Subject Access), patients are entitled to have their own version of events included in their health records.

8 Training and Communication

8.1 Training

Training is necessary to ensure the relevant members of staff have the appropriate understanding in order to satisfy the Information Governance agenda. With suitable guidance, data quality processes will be improved as information will be collected and recorded correctly at the point of entry. This then reduces the requirement for lengthy validation procedures at later dates.

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 allowed to attend the appropriate training courses giving them an adequate level of proficiency in order to carry out their functions effectively.

It is vital that all staff working with clinical and business information have received training on data quality and understand the importance it commands.

8.2 Communication

Copies of this policy will be made available to staff via the policy distribution process.

APPENDIX 1

Data Protection Act 1998 – Principles

A summary of the eight principles of the Data Protection Act 1998 is given below. To see these principles in their entirety, please follow the link below:

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_9#sch1-pt1

Data:

1. Processed fairly and lawfully
2. Processed of specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection