Policy

Policy Guideline

Data Quality Management Policy Guideline

Objective file number: 2011-12910, eA517459
Document classification: For Official Use Only-I2-A1
Policy developed by: Finance and Corporate Services Division
Approved at Portfolio Executive on: 16 February 2012
Next review due: 30 April 2018

Summary The objective of the Data Quality Management Guideline is to facilitate the development and subsequent enterprise-wide adherence to the set of standards regarding data, processes, technologies, workforce competencies and governance arrangements that will be required to achieve the organisation's strategic objectives regarding continuous improvement in the quality of corporate data that is available to support business decisions.

Keywords Data quality management, data standards, data governance, Data Quality Management Guideline

Policy history
Is this a new policy? *N*
Does this policy amend or update an existing policy? *Y*
Does this policy replace an existing policy? *N*
If so, which policies? N/A

Applies to *All SA Health Portfolio*

Staff impact *All Staff, Management, Admin, Students; Volunteers*

EPAS Compatible *Yes*

Registered with Divisional Policy Contact Officer *Yes*

Policy doc. Reference No. G0115

Version control and change history

Version	Date from	Date to	Amendment
1.0	16/02/2012	09/04/2015	Final version endorsed by ED, Health System Performance and PE endorsement
1.1	09/04/2015	Current	Reviewed and updated Risk Management content

Government of South Australia
SA Health

Data Quality Management Policy Guideline

Government of South Australia
SA Health

Document control information

Document owner	Director, Data & Reporting Services, Finance & Corporate Services
Contributors	Senior Manager, ISSQ, Data & reporting Services Director, Information Management, Data & Reporting Services Principle Risk Management Consultant
Document classification	For Official Use Only-I2-A1
Document location	SA Health internet – 'policies page'
Reference	2011-12910, eA517459
Valid from	9 April 2015
Review date	30 April 2018

Document history

Date	Version	Who approved New/Revised Version	Change reference
09/04/2015	V1.1	Director, Data & Reporting Service	Reviewed and updated Risk Management sections
16/02/2012	V1	Portfolio Executive	Original version endorsed by PE

Contents Page

Data Quality Management Policy Guideline

1. Objective

The **Data Quality Management Directive** was the first in a series of documents intended to support the establishment and ongoing operational maintenance of a Data Quality Management Framework that will be required for achieving the organisation's strategic objectives regarding continuous data quality improvement. It provided detailed descriptions of the Guiding Principles that underpin the Data Quality Management Framework as well as provide clear expectations regarding their adoption as part of the organisation's mainstream data management activities. All business units are expected to assess if they are meeting those directives in their data handling practices, especially for data that has a significant impact on the business, such as key corporate collections. Where it is identified that improvements can be made to business process and practices to align more readily with the data quality directives, this document provides practical guidance on *how* to implement changes using 'best practices'. This document assists with both the initial development of an agreed set of standards regarding data, processes, technologies, workforce competencies and governance arrangements as well as achieving and maintaining high levels of adherence to these standards across the entire organisation.

This document is structured to cover each DQMF element in the above order and to provide:

- Detailed description of the element and its role in data quality management; and
- Guidelines for how the elements can be established and then subsequently operationally maintained.

2. Scope

The scope of this document includes:

(a) Data that is used to support decision-making at the following levels of organisational management:

- Health Unit – Data supports a wide range of local **operational** activities including, *inter alia*, the delivery of clinical services to patients, as well as the administration of finances, assets and the workforce. These are collectively referred to as "primary use" as they are the initial reason for collecting the data.
- Local Health Network – Data collected from the monitoring of operational activities for business units across the organisation against agreed performance indicators is subsequently used to inform **tactical** decisions regarding the optimal use of available resources with the aim of maximising efficiencies and effectiveness in business operations.
- SA Health – Data from local systems is used to support a wide range of **strategic** decisions regarding policy, performance, funding and planning that require data collected from across organisational boundaries to be aggregated to create an enterprise-wide view of this data.

Note: Using data to support tactical and/or strategic decision-making is referred to as a "secondary uses" since they are not the "primary use" or reason for why the data is collected.

(b) Each of the elements of the *SA Health Data Quality Management Framework* described in the introduction. (Figure 1 and Appendix A).

(c) Application of the *SA Health Data Quality Management Framework* to both:

- **Business as Usual –** Robust data quality management needs to be established for all existing corporate data collections and associated reporting systems, whereby it becomes embedded within the regular data management activities across SA Health.
- **New data and/or application development** – New data collections and corresponding reporting systems may be required to support new business requirements. There are several stages in the application development process where data quality management interventions need to occur. Ideally, these interventions should be embedded within the Software Development Lifecycle (SDLC) methodology that has been mandated by eHealth for all new ICT system development

3. Principles

A key data management strategic objective for SA Health is to provide users across the enterprise with ready access to information that is known to comply with data quality standards that are required to meet their business requirements.

To meet this objective the Data Quality Management Framework (DQMF) has been developed to support the business in the development of and maintain compliance with agreed enterprise-wide standards regarding data, processes, technologies, workforce competencies and governance for managing data where continuous quality improvement is the goal.

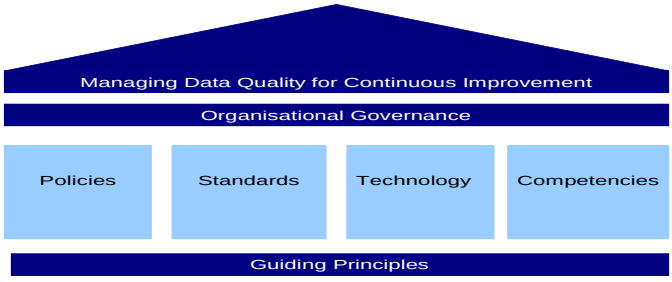

Figure 1: *SA Health Data Quality Management Framework* (DQMF) elements

The elements of the DQMF (Fig. 1) **are:**

- **Guiding Principles:** Statements regarding foundational capabilities required to achieve high-level objectives with respect to improving data quality management.
- **Policies:** Mechanisms for translating these guiding principles into pragmatic, actionable and measurable organisational objectives regarding data quality management, including adherence to standards, monitoring compliance and continuous improvement.
- **Standards:** Definitions of the minimum requirements for data standard, including data definitions and quantitative metrics for assessing quality, as well as for the core business processes and work practices that support data quality management.
- **Technology:** "Tools" that enable execution of data quality management processes and work practices.
- **Competencies:** Workforce competencies necessary for the successful execution of the standard processes for managing data quality in accordance with performance expectations.
- **Organisational Governance:** Defined roles and responsibilities that provide the organisational capability for governance regarding decision rights & accountabilities for data quality management.

4. Detail

This section describes each component of the DQMF with recommendations regarding their establishment and ongoing operational maintenance.

Guiding Principles

Guiding Principle 1: Data quality will be managed with the diligence of other strategic corporate assets.

Data is a valuable corporate asset that is essential in supporting many business functions and activities across the enterprise as well as all levels of organisational management, including operational, tactical and strategic. Poor data quality undermines the value and utility of this important asset as a result of the subsequent negative impacts upon the business activities it supports. Hence, improving and maintaining the quality of corporate data is a strategic priority and will involve measuring and assessing the level of compliance against relevant and agreed quality standards and targets on a regular basis. This will permit all users of corporate data to be assured that it meets all agreed quality standards and that it is fit-for-purpose.

Guiding Principle 2: Data quality management is an enterprise-wide responsibility.

The processing of data from the point of initial capture through to final reporting requires contributions from many individuals and requires collaboration and cooperation across organisational boundaries. All contributors have a shared responsibility in managing the quality of the data they manage.

It is recommended that clear stewardship for data is established within operational business units that are accountable for ensuring that the data they provide to support both local and enterprise-wide reporting, whether for primary and/or secondary purposes, complies with the agreed quality criteria.
Quality behaviours of data collectors, processors, custodians and analysts can also be intrinsically motivated and sustained by receiving feedback and examples of how their contribution assists decision making and service delivery outcomes. If a person attaches meaning to a task and believes their effort is a positive contribution they are more likely to adhere to and refine the prescribed procedures.

It is advisable that staff responsible for data quality management functions be assigned measurable objectives in the development and enforcement of data quality, controls and standards as well as being provided with the context of how the quality of their work impacts the business. They should have access to competency-based training to acquire the relevant skills and knowledge necessary to perform these functions in accordance with the agreed standards and performance expectations.

Guiding Principle 3: Data will be common across the enterprise with regards to definitions, interpretations, formats and business rules for any derived data, unless there is an accepted and documented business justification for deviation.

Standards will be established for all data items and corresponding collections that conform to approved existing standards whenever appropriate. The order of priority for adoption of existing data standards is national, state, inter-state or international.

When existing standards are not available, local standards will need to be developed using the recommended Data Standards Development Procedure that is aligned, where appropriate, with the existing ICT Standards Framework.

Where different collections using data from the same sources require different standards (e.g. data definitions) in order to meet different reporting requirements, the mechanisms used to resolve these inconsistencies should not result in increased burden for data entry, instead, alternative solutions, such as the use of mapping tables, should be implemented where possible and acceptable.

Guiding Principle 4: Data definitions will be unique and stored in a common metadata repository that is accessible via online search.

To facilitate the adoption of existing data standards, they should be made readily accessible from a single metadata repository that is centrally-managed as the only authoritative source. This repository should be searchable online to provide ready access for users seeking information regarding the metadata for any corporate collections and the corresponding data standards.

Guiding Principle 5: All data must be referenced to a single source of truth

To ensure consistency in information wherever and however it is reported across the organisation, it should be from the one authorised "source-of-the-truth". This involves the same data used to meet local "primary-use" business requirements also being used to contribute to enterprise-wide "secondary-use" reporting requirements.

To achieve this objective, wherever possible, transaction data entered into local operational systems should be the source of data used for reporting at all levels of organisational management, from the local health unit, to the Local Health Network and to SA Health. This is represented as a cascade of information reporting requirements at different levels of organisational management that is based upon the unit record transactional data collected as a by-product of service delivery (Appendix B: Corporate Performance Management Reporting Framework).

Guiding Principle 6: Standards need to be established for the execution of data quality management processes and work practices.

Standardised protocols and procedures should be established and re-enforced to ensure the efficient and effective execution of good data quality management processes. Documentation has been developed for the following 5 key data management processes as a guideline for building standards into business-as-usual processes that involve data handling:

- Data Standards Development – Provide clear expectations and guidelines for the development of new data standards and/or amendments to existing data standards that may be required to meet new and/or changing reporting requirements. This methodology complies with the existing ICT Standards Framework (: Data Standards Development Procedure).

- Compliance Checking – Provide clear expectations and guidelines for the regular measurement, monitoring, evaluation and reporting of compliance against pre-defined and agreed data quality criteria. Findings subsequently provide the basis for confirming whether or not data has met with these agreed quality criteria (Compliance Checking Procedure).

- Incident Management - Provide clear expectations and guidelines for managing incidents, which are defined as any "event" that has or may have the potential to negatively impact on data quality that will result in disruptions to the business activities supported by this data. Aim is to rectify any incidents of data quality non-compliance as soon as possible and thereby minimise the risks of disruptions to the business that relies upon this data (Incident Management Procedure).

- Problem Management – Provide clear expectations and guideline (based on the ICT Governance Framework and Incident Management Procedure) for managing problems that are defined as a recurring incident. This involves an investigation into the underlying causes of the incident recurring, implementing changes to prevent recurrence of the incident in the future, as well as verifying that problem has been rectified.

- Change Management – Provide clear expectations and guidelines (based on the ICT Governance Framework and Incident Management Procedure) for managing any changes, planned and/or unplanned, that have the potential to impact upon data quality and any dependent business activities. Any changes to data, applications and/or ICT infrastructure require appropriate impact assessments to be undertaken prior to the changes being approved for implementation. Exceptions may apply when changes are requested by senior executive that need to be implemented within a timeframe not permitted by the standard change management process.

Guiding Principle 7: Address data quality issues "upstream" as close as possible to the point of initial data capture and entry into operational systems.

The principle source of poor data quality is at the initial point of manual data entry into operational systems as a result of typing errors, missing information and/or non-standard entries. Once this problematic data has been entered into operational systems it is difficult to locate and correct. Furthermore, operational data tends to flow from one system to another as part of a multi-step data workflow, whereby the poor data quality proliferates to other systems and impacts upon all business processes that rely upon this data.

An effective mechanism for mitigating these risks is ensuring that all staff responsible for data entry into operational systems has the requisite competencies (knowledge and skills) to minimise poor data entry.

Furthermore, where possible, data quality technologies should be integrated and embedded with operational applications to validate data quality in real-time as it is entered. Other data quality technologies include those for reducing the opportunities for free text entry and requiring data entry operators to select from a prescribed list of approved data values.

Guiding Principle 8: Profile data frequently, broadly, collaboratively and transparently.

Data profiling is a foundational capability for all aspects of data quality management, including continuous improvement, problem resolution and quality assurance. It is not possible to effectively manage data quality in the absence of comprehensive and detailed understanding of its status throughout each of the processing steps from source through to final targets. This involves the following practices:

Data profiling: Measuring and assessing compliance with required data quality criteria.

Data discovery: This helps to avoid the risk of only profiling known data sources whereby previously undetected data quality problems may be identified and prioritised based upon likely business impacts.

Data monitoring: Re-profiling of data as it moves from source through to final targets to retain a history of changes in data quality over time, which is critical for demonstrating progress in achieving the organisation's strategic data quality objectives regarding continuous improvement.

Guiding Principle 9: Data is to be protected from unauthorised access, disclosure and/or modification.

For all SA Health data to be adequately protected against threats to its security, particularly breaches of confidentiality, at a level commensurate with the relevant security requirements and with the obligations for public sector employees stipulated in the Health Act, Mental Health Act and Public Sector Act. This can only be achieved if:

- Personnel who manage this data are aware of its value, confidentiality and need for protection as specified by the *Information Classification and Management Specification*, and handle the data in accordance with the Department's *Code of Fair Information Practice* guidelines.
- Security measures are implemented to ensure that there is a recovery mechanism available if data is lost or damaged and that failover capabilities exist for disaster recovery with critical information systems.
- Disclosure of any SA Health data or information is only done in accordance and compliance with the Department's *Code of Fair Information Practice* guidelines.

This guideline is particularly relevant to the “secondary use” of data. For example, while the “primary” use of clinical data is to support the delivery of health care services to patients, it is also used for “secondary” purposes, such as capacity management, corporate performance management and/or research that will inform health care policy and service planning. This is consistent with a one of the key guiding principles of information management in that reporting at all levels of organisational management should, where possible, be based upon transactional data that was collected as a by-product of service delivery.

Therefore, the intent of the guidelines regarding data privacy protection is not to prevent access to data that is considered confidential and/or sensitive, but to ensure that when access to this data is required for legitimate “secondary uses”, it is managed in accordance with the established data privacy protection principles.

Recommendations

These 9 Guiding Principles (as defined and referred to in the Data Quality Management Directive), if applied across the business, will deliver upon the strategic objective of improving the quality of information available to support better business decisions. There are two key aspects to keep at in mind when implementing these Guiding Principles in an operational environment:

- All of the data, people, processes and technologies associated with the end-to-end flow and processing of data from source systems through to final targets should be closely aligned with the relevant Guiding Principles.
- All stakeholders contributing to the flow and processing of data need to have a working knowledge of these Guiding Principles as well as an understanding of how they impact of their data management activities and practices.

Organisational Governance

Organisational governance structure and processes are required for both the initial establishment and subsequent maintenance of the levels of adherence to the set of agreed enterprise-wide standards regarding data, processes and technologies that are required for the organisation’s data quality management objectives to be achieved. They provide the environment for administering the data workflows and associated quality management activities that comply with agreed standards through regular status monitoring and reporting.

Consistent data work-flow processes and work practices that focus on data quality priorities start with well-defined roles and responsibilities for data quality management within the organisation and their assignment to the relevant stakeholders contributing to the end-to-end processing of data from its original source through to the final output.

Critical success factors for ensuring that all stakeholders effectively contribute towards achieving the organisation’s data quality objectives include:

- Clear definition of the functional roles and responsibilities that contribute to data quality management along with expectations regarding levels of performance (see Appendix F for detailed Responsibility Matrix);
- Formal acknowledgement and recognition of these roles and responsibilities as part of their normal duties by local management; and
- Access to the competency-based training required for them to acquire the knowledge, experience and technical skills necessary to successfully perform their roles and responsibilities to the levels of performance expected.

The recommended approach to implementing and maintaining effective organisational governance is to use multi-functional teams (MFTs) with representation from key stakeholder groups. Members of the MFT are assigned clearly defined roles and responsibilities.

Stakeholder Roles and Responsibilities

The key roles and responsibilities for managing data quality include:

Data Entry

Functional Roles

Data entered and/or updated in the local operational systems is the initial point of data capture. This may occur during patient registration and/or admission, as well as subsequent updates (additions, deletions, modifications) by authorised administrative and/or clinical staff.

Staff entering and/or updating data in these systems are responsible for ensuring that it complies with agreed data quality criteria.

Responsibilities

To ensure data entered into operational systems meets agreed quality criteria, all staff authorised to enter and/or update data are responsible for maintaining a working knowledge and understanding of:

- How the data entered into local operational systems has both a “primary” and “secondary” use, as well as the likely impacts on these uses as a consequence of poor data quality.
- Data quality criteria that apply to the data they are responsible for entering and/or updating into local systems, as well as expectations regarding levels of compliance to these criteria.
- Role and use of a metadata repository as the authoritative reference source for information regarding the data standards that apply to the data they enter into local systems.
- Standardised procedures associated with each of the core data quality management processes, as well as their roles and responsibilities. These processes include regular monitoring of data quality and the subsequent management of incidents, problems and/or changes as required.
- Role and responsibilities in contributing to the design, implementation & testing of any changes to work practices and business processes that are recommended for resolving recurring problems related to errors with data entry.

Data Provider

Functional Roles

Ensuring that the data available from their organisation’s local operational systems meets the agreed data quality criteria that are required for both the “primary” and “secondary” uses of this data. This is an important role since this is the source of data that (ideally) is used to meet all reporting requirements, in accordance with Guiding Principle 5.

Responsibilities

To ensure that the data available from local systems complies with the agreed data quality criteria, it is recommended that Data Providers:

- Undertake regular data quality checks that the data available from their operational systems complies with agreed quality criteria in accordance with a Compliance Checking Procedure with the findings documented in a Data Quality Compliance Report that is made available to other stakeholders.
- Provide a single interface between the Department and their organisations for resolving any issues regarding data quality compliance, which would involve coordinating appropriate corrective actions, as and when required, in responding to any incident, problem and/or change management in accordance with corresponding recommended baseline procedures (i.e. Incident Management Procedure, Problem Management Procedure, Change Management Procedure).

Data Custodian

Functional Roles

Role of the Data Custodian includes managing the quality of data within the corporate collections and confirming that it meets all of the quality criteria required for its subsequent use.

Data Custodians are also responsible for ensuring that the business and technical metadata that is available from the metadata repository regarding their corporate collection is complete, accurate, consistent and up-to-date.

Responsibilities

To ensure that the quality of data in the corporate collections meets with agreed data quality criteria, Data Custodians are advised to:

- Conduct regular monitoring of data quality compliance for the corporate collections for which they are responsible in accordance with a Compliance Checking Procedure.
- Provide a single interface between the Department and the health units (via the Data Providers) for resolving any issues regarding data quality compliance. This would involve coordinating appropriate corrective actions, as and when required, in responding to incident, problem and/or change management in accordance with corresponding recommended baseline procedures (i.e. Incident Management Procedure, Problem Management Procedure, and Change Management Procedure).
- Assume the role of a “Registration Authority” when using the metadata repository to support the development of new and/or amendments to existing data standards relevant to the corporate collections for which they are responsible. This involves coordinating the activities of stakeholders (Working Group) in developing the data standards specifications and preparing the necessary documentation for seeking authorisation of the new and/or amended standard in accordance with the recommended Data Standards Development Procedure and the ICT Standards Framework.
- Conduct regular reviews of information published in the metadata repository regarding the corporate collections for which they are responsible to ensure it is accurate, complete and up-to-date.

Data Quality Manager

Functional Roles

Functions include:

- Custodian of all data quality management and improvement strategies, policies, standards and procedures from definition and design through to execution and evaluation.
- Increasing awareness, understanding and adoption of agreed enterprise-wide standards by all parties responsible for data quality management throughout its complete lifecycle.

Responsibilities

To facilitate the successful adoption and operational implementation of a *SA Health Data Quality Management Framework* across SA Health, the Data Quality Manager will:

- Coordinate the development of any new enterprise standards and/or amendments to existing enterprise standards for data, processes and technologies in accordance with Data Standards Development Procedure and ICT Standards Framework.
- Develop and implement communication and corresponding change management strategies to support the successful adoption of new business procedures and workflows regarding data quality management and improvement.
- Liaise with relevant parties as required to assist with resolving any data quality issues.

Executive Sponsor

Functional Roles

Role of the Executive Sponsor is to facilitate the setting of strategic directions with regards to data quality management, while providing visible executive and senior management support for data quality improvement initiatives, as well as ensuring adequate resources for these initiatives.

Responsibilities

To ensure that strategic directions with regards to data quality management remain closely aligned with corporate business strategy, the Executive Sponsor should:

- Set initial direction and goals for the data quality improvement initiative.
- Approve data quality management and improvement policies and track the progress of data quality improvement initiatives compared to target plan.

In providing visible executive and senior management support for data quality management initiatives, the Executive Sponsor will:

- Ensure execution of the data quality management policies.
- Review and prioritise projects, determine funding needs and request funding.
- Seek senior executive endorsement and mandate for implementing data quality management initiatives in accordance with the existing ICT Governance Framework.

It is recommended that The Data Management Advisory Group (DMAG) functions as a Specialist Advisory Group under the SA Health ICT Governance Committee structures in providing specialist advice regarding the impact of ICT initiatives on the organisation's data quality objectives and the flow-on effect upon business operations. As Chair of the DMAG, the Executive Sponsor could be responsible for reporting to SA Health executives as required, which would include:

- ICT Steering Committee – approve investments and prioritisation of enterprise-wide data quality initiatives in accordance with the strategic objectives of SA Health.
- ICT Clinical Reference Group – provide clinical leadership, direction and endorsement of data quality initiatives that impact upon the quality of information available from local operational systems used to support delivery of health care services to patients (i.e. "primary use")
- ICT Business Systems Group – provide business and corporate leadership, direction and endorsement of data quality initiatives that impact upon the quality of information available to support corporate and business decisions across SA Health (i.e. "secondary use").

Implementation using Multi-Functional Teams

To better integrate and coordinate activities of the key stakeholders including Data Entry, Data Provider, Data Custodian and Data Quality Manager, the following guidelines are recommended:

a) *Bring together a multi-functional team (MFT) for your key data management processes.* The design, development and subsequent enterprise-wide adoption of agreed standards for data and/or processes requires a high level of effective communication, collaboration and cooperation between all stakeholders contributing to the end-to-end flow and processing of data from source systems through to final targets. MFTs are an effective mechanism for achieving these objectives because there can be representation from all of the key stakeholders groups that contribute to a dataflow and process, whereby they have a shared responsibility for data quality management.

b) *Establish an MFT for each of the key corporate collections.* This is highly recommended. Their key role would be to reach agreement on standardised protocols and procedures for each of the core data quality management activities including: development of new data collections to respond to new reporting requirement; conducting regular data quality compliance checks; and, responding to any incidents, problems or changes that impact upon data quality for their collections. Examples for each of these procedures have been developed and could be modified by the MFT to develop standardised procedures that are customised to meet their specific needs.

c) *Utilise existing forums.* An MFT is not necessarily a new group. If groups and processes are already in place and are effectively managing operational issues, then existing people can be assigned data quality management roles for appropriate operational areas. Using existing forums is recommended, however if there is not a suitable forum or group in place, then an MFT can be brought together to look at what needs to be addressed in that area of the business to align more closely with the 9 Guiding Principles.

d) *Define 'who' will fulfil the key roles.* Once all stakeholders have agreed on a standardised procedure, it is recommended that the MFT translates the "operational" model into an "organisational" model by identifying those who will be responsible for operational implementation of these procedures. They should be embedded within the normal data management activities whereby they become additional roles and responsibilities for existing staff.

Key stakeholder groups

The stakeholder groups represent different levels of organisational structure from individual health units, to Local Health Networks, metropolitan and country regions to finally the SA Health enterprise.

The recommended key stakeholder groups that should be represented in the membership of any MFT should include as a minimum:

- Health Unit
  - Administrative staff that enter and/or update patient and/or administrative data into operational systems that are a data source for corporate collections. Representation at the local health unit level would be via the Administration Manager to whom they would normally report.
  - Medical staff that enter and/or update data into the same local operational systems. Their representative at the local health unit level would be the administration manager or patient information manager depending on the structure of that particular hospital.
  - Medical Records Managers are responsible for medical records clerks, clinical codes reporting, records retention and often medical records department operations within the local health unit, as well as assuming the role as the (Enterprise Master Patient Index (EMPI) Coordinator.

- Local Health Network / Country Hospital Cluster
    - Corporate Services Managers are assigned to each of the LHN (for metropolitan) or hospital cluster (for CHSA) and are responsible for, *inter alia*, health information services, including medical records, clinical coding and admissions. They perform the role of Data Providers in ensuring that the data available within operational systems across their LHN/Hospital Cluster complies with agreed enterprise-wide data quality standards that are required to meet both primary and secondary reporting requirements.
- Regional (Metropolitan vs. Country)
    - The Corporate Service Managers assigned to each of the metropolitan LHNs report to the Business Account Manager (BAM). Similarly, the Corporate Service Managers assigned to each of the Country Hospital Clusters report to CHSA's Director, Business Development. Hence, the role of the BAM and CHSA Director, Business Development, within the MFT is to provide a regional representation and to ensure consistency across all of the LHN / Country Hospital Clusters within the metropolitan and non-metropolitan regions respectively.
- SA Health
    - The data quality management interests of SA Health are represented by the Data and Reporting Services branch(D&R), which is responsible for managing many of the corporate collections that provide data to support most of the mandatory reporting requirements, especially from a whole-of-enterprise perspective.
    - The Information Assembly team within D&R assume the role of Data Custodian for the corporate collections by ensuring that the data in these collections that is sourced from local health units complies with the agreed data quality criteria that need to be met for meeting all subsequent reporting requirements.
    - Information Delivery team within D&R is responsible for, *inter alia*, ensuring the quality of information that appears in any of the reports that are used to provide access to this data across the enterprise. This data is sourced from the corporate collections and stored in the Central Data Warehouse (CDW) in a structure that is optimised for reporting.
    - Information Systems, Standards and Quality team within D&R is responsible for promoting consistency in the use of data standards across all data collections.

These key stakeholder groups, their data quality management roles and responsibilities, as well as recommendations regarding their representation on the MFTs are summarised in Appendix D. By using MFT methodology you can bring the right people together to put into place and maintain organisational governance for data quality management as part of the DQMF.

Policies

Policies serve as the mechanisms for translating guiding principles into pragmatic, actionable and measurable strategic objectives for the organisation, such as the continuous improvement in the quality of corporate data. More specifically, they direct the formal development of agreed standards (for both data and processes) as well as their adoption across the enterprise that is required to achieve these strategic information data quality management outcomes.

The key policy document is the Data Quality Management Directives which describes the 9 key guiding principles as 'Directive Principles'.

It is recommended that:

- All of the data, people, processes and technologies associated with the end-to-end flow and processing of data from source systems through to final targets should be closely aligned with the relevant Data Quality Management Directives.

- All stakeholders contributing to the flow and processing of data need to have a working knowledge of these Data Quality Management Directives as well as an understanding of how they impact of their data management activities and practices.

In addition to having these detailed 'Directives', this 'Guidelines' document (Data Quality Management Guidelines) is an aid to practical implementation of the directives. Supporting these two core documents are five baseline procedure documents providing guidelines on achieving best practices for data quality management at an operational level. They include: Data Standards Development Procedure, Compliance Checking Procedure, Incident Management Procedure, Problem Management Procedure & Change Management Procedure)

Standards - Data

Adherence to agreed enterprise-wide data standards is essential for improving the quality, relevance and consistency of information available to better support business decision making and is a key element of the DQMF.

There are several fundamental competencies of data that benefit from standardisation and consistency. These competences are primarily more relevant to areas of the business where managing data is core business activity. .

However, ensuring data is fit-for-purpose is relevant to all business units and therefore these guidelines regarding Data Quality Assessment Criteria is relevant to all.

Foundational Competencies

It is recommended that the following competencies of Data Definitions, Metadata, Data Set Specifications, Minimum Data Sets and Common Data Structures are established to promote compliance with enterprise-wide data standards:

Data Definitions

Common terminology and definitions are required for all data elements held in corporate collections to ensure consistency in their meaning, use and interpretation. Where possible, these data definitions should be consistent with other national standard classifications to ensure overall compatibility with national data. This includes the National Health Data Dictionary published by the Australian Institute of Health and Welfare (AIHW) that contains standard data elements and definitions for use in any Australian health, housing and/or community data collections.

When national data standards do not already exist, the hierarchy in descending order of priority for adopting existing standards is:

State definitions

Interstate definitions

International definitions

Locally developed data definitions

Metadata

Metadata extends the information provided by Data Definitions to include detailed structured description of the content, quality, condition or any other characteristics of data that are important for its management and use. It enables all those collecting, using and exchanging data to share the same understanding of its meaning, representation and derivation. This promotes the correct use and interpretation of the data. Metadata that has been formally endorsed for use across the enterprise are subsequently referred to as Data Standards.

Data Set Specifications

Data Set Specifications (DSS) contain a list and corresponding descriptions of the data elements that are used within specific data collections and are required for each of the Department's corporate collections.

Minimum Data Sets (National and Local)

National Minimum Data Set (NMDS) is a minimum set of data elements agreed for mandatory collection and reporting at a national level. It represents national agreement to collect uniform data and to supply it as part of the national collection. The National Health Data Dictionary (NHDD) contains the definitions for the data elements that are included in the NMDS for the health sector.

Common Data Structures

The National Health Information Model (NHIM) defines the information structure underlying the diverse processes and policies of health care delivery. It was developed and is maintained by the Australian Institute of Health and Welfare on behalf of the National Health Information Management Group (NHIMG) and the National Community Services Information Management Group (NCSIMG). The NHIM enables related data elements from the NHDD to be grouped under a single entity rather than alphabetically, where entities are the "things" about which we need to know or hold data on, such as people, places, objects or events.

Data Quality Assessment Criteria

Many different measures are used to assess data quality depending upon the users' perspective. The following is a hierarchical framework for organising data quality dimensions that are most important to the business users of the data

Intrinsic DQ – data must be accurate, correct, objective and from reputable sources.

Contextual DQ – data must be relevant and timely for use to support the intended business requirement.

Representational DQ – data must be in a format that is readily interpreted by the user.

Accessibility DQ – data must be accessible to the user via "tools" that are customised to their requirements and technical competencies.

If the data management strategic objective is to ensure that the information available meets the organisation's business requirements, then appropriate data quality criteria should assess whether it is "fit-for-purpose". They provide the benchmarks for measuring and monitoring levels of compliance with agreed data quality requirements necessary to support the business.

The recommended minimum criteria for assessing data quality are listed in Appendix C and it is advised that all areas have agreed criteria for their data that should be met and monitored though a compliance checking process (e.g. Compliance Checking Procedure).

Recommendations

To ensure your area has 'standards' for foundational capabilities of data, the following steps are advised for those areas of the business where data management is the core business.

a) Through MFTs, for each of the corporate collections, undertake to:

- Evaluate the extent to which each of the foundational capabilities listed above (section 5.6.1) and that are designed to ensure greater compliance of the corporate collections with agreed quality criteria have been established; and
- Plan and support the implementation of a work programme aimed at establishing these foundational capabilities if they do not already exist.

- Develop a communication strategy aimed at providing all relevant stakeholders with regular updates on progress with implementing this work programme.

b) Steps involved would include:

- Determine and document nature and extent to which these foundational capabilities have been established for the corporate collection. This would include:
    - Identify the data items for which agreed and approved Data Definition standards already exist and conversely, those for which approved standards are not available.
    - Where approved data standards already exist, determine whether they have been adopted for use in the corporate collection, while also documenting incidents and corresponding explanations for why existing data standards have not been adopted.
    - Determine whether the data items for which standards already exist have been published and made available from the SAHMR (or other appropriate metadata repository).
    - Determine whether a Data Set Specification exists that lists all of the data items contained within the corporate collection. If so, then determine that this information has been made available via SAHMR.
    - Determine and document the information reporting requirements that are supported by the corporate collection(s). This would include descriptions of their Minimum Data Sets (MDS) and identification of those that use data from the corporate collections. This information is to be made available via the SAHMR.
- Developing and implementing a program of work to address any of the following issues identified by this assessment of the current state. These may include:

Developing and seeking endorsement of new data standards for the data items for which existing standards are currently not available. This should be done in accordance with the recommended Data Standards Development Procedure. Furthermore, a key element of this recommended methodology is the collaboration between the members of the MFT during this development process.

- Promoting adoption of existing data standards where they already exist but not applied to corporate collections. This will require analysis of the reasons provided for why existing data were not adopted.
- Ensuring that the metadata available from SAHMR regarding the corporate collections is accurate, complete and up-to-date.

- Communications strategy is developed and implemented to inform all relevant stakeholders of:
    - Audit findings, particularly with respect to:
        - Identification and description of the data standards that are relevant to the data within the corporate collections and that is sourced from the local operational systems.
        - Proposed program of work to be undertaken to develop new standards as required.
    - Role of the SAHMR as gateway to access information regarding both existing standards as well as progress in the development of new standards.

Standards - Processes

Processes provide procedural direction over how organisational governance will operate. This includes effectively governing the management of data quality throughout its entire lifecycle, including clear guidelines and accountability for compliance checking, incident, problem and change management, impact assessment and stakeholder communications.

Standardisation of these processes will deliver the following inter-dependent benefits:

- Ensure greater consistency, reliability, efficiencies and effectiveness in how they are implemented by formalising underlying workflows and work practices;
- Greater understanding and agreement on the specific roles and responsibilities for those contributing to these data quality management processes;
- Better understanding of the nature and extent of knowledge and skills required by stakeholders to effectively and efficiently fulfil their respective roles and responsibilities that assists in the design and delivery of education and training programmes customised to equip the workforce with these required competencies.

Standardised procedures are recommended for operational implementation of the following the processes:

- Data Standards Development Procedure
- Compliance Checking Procedure
- Incident Management Procedure
- Establishment of a problem management procedure
- Establishment of a change management procedure

Data Standards Development Procedure

The development of data standards is integral to the creation of new collections to meet new reporting requirements. New data standards may also need to be developed for existing data collections where none are already available. Furthermore, data standards may need to be changed over time. Hence, operational procedures need to be established for the development of new and/or modification of existing data standards to ensure that they become a key component of the data development process, as well as to ensure their ongoing relevance and maintenance.

Recommendations

MFTs established for each of the corporate collections undertakes the following activities:

- Review, update and agree to adopt the recommended Data Standards Development Procedure when developing new and/or amending existing data standards that apply to the corporate collections for which they are responsible.
- Promote the use of the SAHMR (or other appropriate metadata repository) to support the collaboration and cooperation between all relevant stakeholders when using this procedure by developing and supporting a work program aimed at raising awareness regarding SAHMR as well as ensuring that all relevant stakeholders have access to training regarding the use of SAHMR in standards development.

Steps involved would include:

- From the outcomes of the checks of existing Data Standards recommended, process those data standards and Data Set Specifications (DSSs) through the agreed Data Standards Development Procedure to gain appropriate endorsement as a SA Health standard. This would apply to the following items;
    - Agreed and approved standards are not available.

- Part of key corporate collections where standards already exist but have not been published and made available from the SAHMR.
- Necessary documentation does not exist regarding descriptions of their Minimum Data Sets (MDS) and identification of those that use data from the corporate collections.

- Adopting the key principles of the Data Standards Development Procedure which are;
  - All changes to Data Standards and DSS that involve either changes to existing items or creation of new items should all go through the same Data Standard Development Procedure and use the SAHMR system as the tool to govern the process.
  - Data Stewards take responsibility for documenting the details and instructions and permissible values to meet the necessary standard as determined in the Registrar Check list to ensure full, clear, instructive standards are created.
  - Implement a two stage approval process:
    - By the Registrar who takes responsibility for preparing all of the necessary documentation for seeking formal approval of new and/or changes to data standards in accordance with the ICT Standards Framework
    - Forwarding request for formal approval of the proposed new and/or amended standard to the appropriate authority in accordance with the ICT Standards Framework.
- All changes to existing standards should be used as an opportunity to ensure all documentation and the ability to monitor data compliance with agreed standards is up to the required level in accordance with the Registrar Checklist. Due diligence should be undertaken to identify data items and corresponding standards that may not have gone through the same rigorous process required for them to be recognised as a SA Health standard.
- Dissemination of information around new and/or changed standards should be the responsibility of the MFT to ensure impacted areas are aware of new and changed data standards. This mechanism should be part of the change control procedure documentation.
- Changes that need to be fast-tracked, such as ministerial directives, should nevertheless still follow the same procedure with only a minor difference being a streamlined authorisation process. Any new standards resulting from this process should still be full, complete, and robust to meet the same level expected of any other standard.
- Operational managers involved in data management should endorse and promote the use of the process with their teams and manage non-compliance with the procedure in their unit.
- Communication of the procedure to health units so there is an awareness of the mechanism for how new and changed items are managed and to enable them to expect communications regarding changes and new Data Standards that they will then be required to act upon to ensure compliance.

Note: Examples of current existing standards and guidelines are provided in *Appendix H Operational Manuals & Standards F&PE*. In addition the *South Australian Cancer Registry Notification Manual* can also be used for reference.

If, as part of your assessment of compliance with the 9 Directive Principles, a gap is identified whereby a data standards development procedure is needed, use of the example document Data Standards Development Procedure is recommended. This will provide a baseline to work through as an MFT.

Compliance Checking Procedure

Compliance against agreed standards is relevant across all part of the business and is one of the most important tools with regards to enable data quality excellence.

It is not possible to manage data quality unless it can be readily, accurately and reliably measured. Hence, effective and efficient data quality management requires ready access to quantitative information regarding the current status of data quality. This requires formalised and standardised procedures to be established for the regular monitoring, measurement, evaluation and reporting of compliance of data against pre-defined quality criteria Findings from compliance checks subsequently provide the basis for confirming whether or not the data has met agreed quality criteria and thereby "fit-for-purpose" with respect to its intended use(s). Furthermore, the reporting of any issues regarding data quality non-compliance detected during these checks will be a trigger for initiating the Incident Management Process that is intended to rectify the issue as soon as possible to minimise any potential negative impacts on the business supported by this data.

Key steps in the data flow where regular data quality compliance checks are recommended would include:

1. Data Entry

   In accordance with the key Guiding Principle that any data errors should be addressed "upstream" and as close as possible to the point of initial data capture and entry into the information system, regular data quality compliance checking should be undertaken for data entered into local operational systems.

   Criteria for assessing the quality of data entered into local operational systems must relate to both the "primary" intended use, as well as any "secondary" use.

2. Data Integration

   Data entered into local operational systems from across multiple sites needs to be integrated to create an enterprise-wide view. This generally involves some transformation (or "cleansing") of the data so that it complies with a common data standard format as an essential prerequisite to it being integrated. Data quality compliance checking of data is required after it has been extracted, transformed and integrated (generally referred to as the "Staging" environment) to verify that the business rules for cleansing, standardising and integrating the data have been successfully executed.

3. Data Warehouse

   Once integrated, further processing of the data is generally required so that its structural representation is optimised for reporting. This involves the corresponding movement of data from Staging to the Data Warehouse environment, where the data structure is optimised for fast query and retrieval of data.

   This is a critical success factor for the design of information reporting systems that provide access to low latency data required to support near real-time decision making, such as optimising patient flows during periods of high demand. Hence, regular data quality compliance checking of the data held within the Data Warehouse is required to verify that no data errors have occurred during its migration and transformation from Staging to the Data Warehouse.

4. Data Presentation

   A final step in the processing of data is its presentation to the user in the final output, which will vary depending upon the reporting application. Data displayed in these final outputs is retrieved from the Data Warehouse in response to a query executed by the user through a query and reporting tool, such as Business Objects. Hence, regular data quality compliance checking of data displayed in final outputs is required to verify that the correct data is retrieved and displayed. This is particularly relevant when the data displayed in the final output is "derived" through complex calculations involving a number of different data items. Regular checking is required to ensure that these calculations are executed in accordance with the agreed business rules for creating each of the derived measures.

Recommendations

It is recommended that MFTs develop and agree on a standardised Compliance Checking Procedure for each of the corporate collections and determine how it is to be incorporated within the regular data management activities. This would involve completing the following tasks:

(a) Planning a compliance checking regime

Prepare documentation detailing the following:

- Mapping of the end-to-end flow of data from its initial point of entry into local source systems within health units through to final targets. This process flow map will include all of the individual steps in this end-to-end processing of data and provide detailed descriptions of each step with regards to: inputs, including their source, processing performed on inputs, outputs produced and targets; stakeholders contributing to and/or executing these processes; and, the technologies (if any?) used by stakeholders as enablers for executing these processes.
- Identification of the steps involved in this end-to-end data flow / processing where data quality management interventions are to be applied for monitoring and assessing compliance with expected data standards ("check-points"). The steps selected as compliance "check-points" will generally be associated with the movement of data between different physical locations and/or any associated data transformations that may be automated or involve manual interventions.
- Description of the data quality compliance requirements for each of these "check-points". This will include detailed descriptions of the data quality criteria to be used to assess compliance, which will vary between "check-points" depending upon how the data is processed and/or transformed. For example, simple profiling of data to detect any changes through before-and-after comparisons may be appropriate when data is simply moved between physical devices. However, when steps involve data transformations such as in the calculation of derived measures (e.g. KPI), and then more complex analyses may be required to verify that the associated business rules have been correctly implemented.

  The MFT should determine the frequency with which these checks are conducted. This will depend upon the volatility of the data or the frequency with which it changes, subject to the agreed re-fresh cycle for the data. When data is used for annual reporting, any new data may only be processed every 12 months. Conversely, data used for near real-time reporting would be refreshed more frequently (e.g. every 30 minutes). Under these circumstances, there is a very brief timeframe for checking data quality and responding to any problems if detected. Hence, emphasis must be on optimising the quality of data upstream at the initial point of data capture and entry into source systems.
- Determine frequency and requirements of data quality audits. Unlike the regular checking of compliance as part of ongoing data management activities, these audits represent an ad hoc check of compliance at each of the individual check-points within the complete dataflow from source to final target. The MFTs can to provide direction on how often ad hoc audits should take place on particular collections and what those audits should be targeting. Outcomes of data quality audits should trigger problem management processes.
- Description of the standard reports for recording data quality compliance checks and audit findings that are used to inform other stakeholders of these findings on a need-to-know basis. These reports serve a number of purposes including: confirming that data meets the quality criteria and expectations; initiating an incident or problem management process aimed at rectifying any data quality problems detected during the quality check and/or audit; and, providing a historical record of the progressive improvements in data quality for the corporate collections that have been achieved following the establishment of the *SA Health Data Quality Management Framework*.
- Description of the operational model for how the data quality compliance checking is to be implemented that includes detailed descriptions of:
  - Business processes, workflows and tasks associated with:
    - Conducting the data quality compliance checks at each "check-point" and the

subsequent reporting of the results;

- Protocols for notifying other interested parties of any incidents of non-compliance;
- Activating and executing pre-determined problem escalation strategies aimed at resolving any issues of non-compliance; and
- Communication updates regarding problem resolution.

o Enabling technologies ("tools") that support these compliance monitor activities, including:

- Data profiling and benchmarking against data element standards published in the metadata repository as part of the data quality assessment criteria;
- Reporting of findings, especially notifications for incidents of non-compliance; and
- Data cleansing.

- Mapping of this operational model to the current organisational model for relevant business units for the stakeholders represented in the MFT. This will involve assigning new roles and responsibilities to existing staff within these units. This serves to embed an ongoing discipline of standardisation, ownership and accountability for managing data quality as part of the regular data management activities. This assignment of roles and responsibilities is best summarised as a responsibility (RACI) matrix that defines the following for each of the operational tasks that need to be performed:

  o Responsibility – Who is responsible for performing the task? *(e.g. Who is responsible for implementing the regular compliance checks and/ or the ad hoc audits?)*

  o Accountability – Who is accountable for ensuring that these tasks are successfully performed? *(e.g. Who manages the staff responsible for implementing the compliance checks and ensures that they have the time and resources necessary to perform these duties in accordance with performance expectations.)*

  o Consultation – Who needs to be consulted regarding the execution of the task? This may involve seeking advice and/or guidance from others. It may also involve requesting approval to execute the tasks? *(e.g. Who needs to be contacted to confirm that the most recent data refresh cycle is completed and that new data is ready for testing?)*

  o Inform – Who needs to be informed about execution of the process? *(e.g. Who needs to be notified that a compliance check has been successfully conducted and of its findings?)*

It is recommended that a Compliance Checking Procedure is developed and agreed to by the MFT for each of the corporate collections. The procedure developed for the new ISAAC reporting system could be used as a model for developing and implementing similar procedure for other reporting systems and associated corporate collections (Compliance Checking Procedure for New ISSAC)

(b) Implementing Compliance Checking

Compliance checking procedure agreed to and endorsed by the MFT is to be implemented and assessed with respect to operational effectiveness and efficiency in confirming the quality of data at each of the designated "check-points", identifying any issues, notifying all other interested parties, and more specifically, initiating an incident management response as required.

It is essential that the Compliance Checking Procedure is considered as an integral component of the regular data management workflows (i.e. business-as-usual) for this assessment, as opposed to being considered as a "once-off" activity that is only undertaken occasionally as required. Ad hoc audits are recommended to capture a 'snap shot' view of how an end-to-end dataflow process is performing at a particular date and time and to trigger problem management processes.

(c) Review

Document that details findings from the assessment of the initial implementation of the Compliance Checking Procedure that could be used to suggest any modifications to the procedure to improve its efficiency and effectiveness. The development and subsequent adoption of any standardised processes is an iterative process in which progressive improvements are made based upon

feedback from previous experiences.

(d) User Guide

Document for providing detailed instructions for implementing a data quality Compliance Checking Procedure that would include:

- Description of the steps involved in the design and develop of a procedure for the regular monitoring of data quality (as per [a] above); and
- Brief description of the major problems that are likely to be encountered when implementing a data quality compliance checks within both the SDLC & BAU processes, along with suggested problem resolution strategies.

If, as part of your assessment of compliance with the 9 Directive Principles, a gap is identified whereby a compliance checking procedure is needed, use of the example document Compliance Checking Procedure is recommended. This will provide a baseline to work through as an MFT.

Incident Management Procedure

A standardised procedure is recommended for managing incidents, which are defined as any "event" that has or may have the potential to negatively impact on data quality with subsequent flow-on disruptions to the business activities supported by the data.

The aim of Incident Management Procedure is to quickly rectify any data errors detected so that the risk of disruptions to business operations are minimised. Ideally, the aim is to rectify these errors before they impact on any downstream business operations. If not, then these procedure needs to include protocols for notifying stakeholders downstream of details regarding the incident so that they can implement their own contingency plans.

Recommendations

It is recommended MFTs develop formal procedures for resolving any data quality incidents that are detected from whatever source, but especially from the regular compliance checks.

Essential requirement of this procedure include:

- All relevant stakeholders need to be readily and effectively notified of any incidents so that corrective actions are instigated as soon as possible to minimise the risk of any downstream impacts. This means bi-directional notifications (where applicable):
  - stakeholders upstream need to be notified in case their activities have contributed to the data quality incident as well as being provided with sufficient information to assist with identifying the incident and investigating possible causes and corrective actions; and
  - stakeholders downstream need to be notified so that they can assess likely impacts as well as take steps to mitigate them where possible.
- Standard templates should be used for all incident notifications to ensure both consistency and completeness in the information exchanged, as well as ensure that the content meets the requirements of all recipients, both upstream and downstream. Another benefit from use of standard incident notification template is the reduction in time to create and distribute these notifications.
- The complete lifecycle for responding a data quality incident from initial detection through to final resolution should be documented in detail in an Incident Record. Hence, all stakeholders directly involved in managing an incident are required to update this Incident Record such that it accurately records the current status of progress in resolving the data quality incident.
- Standard template should be used for an Incident Record to obtain the same benefits mentioned above for incident notifications. It is recommended that the same standardised template be used for both the incident notifications and creating an Incident Record.
- Corrective actions for managing incidents should be based upon the following steps:

- Analyse – Identify the error; investigate to diagnose the cause; decide on corrective actions
- Implement – Undertake corrective actions to rectify the error
- Monitor – Check and confirm that corrective actions have successfully rectified the error.

If, as part of your assessment of compliance with the 9 Directive Principles, a gap is identified whereby an incident management procedure is needed, use of the example document Incident Management Procedure is recommended. This will provide a baseline to work through as an MFT.

Problem Management Procedure

An Incident Management Procedure deals with resolving single events that were unexpected and previously unknown. Ideally, once rectified, the same incident should not recur. However, if similar incidents were to be detected, this would indicate a possible problem with the underlying flow and processing of the data. Under these circumstances, standardised workflows need to be implemented with the aim of preventing the recurrence of incidents and minimising the likelihood and severity of impacts on business operations that use this data.

The first step in a problem management procedure involves conducting a comprehensive and detailed root-cause analysis to identify and better understand the contributing factors. Findings subsequently inform decisions regarding the changes / improvements to the people, processes and/or technologies that will be required to ensure the incident does not recur.

Recommendations

It is recommended MFTs develop a Problem Management Procedure that provides clear expectations and guidelines for managing data quality problems, which includes:

- Investigation into the underlying causes of incidents;
- Implementing changes to prevent the recurrence of incidents in the future; and
- Verify that the problem has been successfully resolved.

The structure of the process map for the Incident Management Procedure was designed primarily to illustrate the protocols for communication (notifications) between all stakeholders involved in the end-to-end processing of data from source to target, as well as across the organisational levels of management, from individual health units, through LHN to Central Office. However, the process map required for a problem management procedure differs in that it identifies the key roles associated with problem resolution, which includes:

- Problem Manager – responsible for process management; accessing necessary resources; coordinating activities; quality assurance
- Support Group – provide access to the technical knowledge and skills required to support problem investigations, as well as design and implementation of corrective actions.

Those assigned responsibility for these roles will depend upon the stage in the end-to-end processing of data where the problem occurs. For example, if preliminary analyses indicate that the data quality problem originates from point of initial data entry, then the roles of Problem Manager and corresponding Support Group with be assigned to staff that are responsible for data entry.

If, as part of your assessment of compliance with the 9 Directive Principles, a gap is identified whereby a problem management procedure is needed, use of the additional guidance in the appendix is recommended. This will provide a baseline to work through as an MFT.

Change Management Procedure

A key challenge in being able to successfully manage corporate information so that it continues to support the organisation's business requirements is in being able to respond and adapt to the many changes that have the potential to impact upon data quality and hence its value in supporting the business. The key sources of change include additions, deletions and/or modifications to any of the following: ICT Systems, Data Entry, Business Requirements and Data Standards

A good change management procedure provides clear expectations and guidelines regarding formal processes for managing any changes that have the potential to impact upon data quality with the aim of minimising the risk of any subsequent business impacts. It provides a structure to support the governance of change management so that:

- Changes are authorised before any costs are incurred in building and testing the change;
- Technical and business impacts of any proposed change are assessed and authorised prior to change being implemented; and
- Risks associated with any change activity are identified, assessed and proactively managed.

Recommendations

It is advised MFTs develop a Change Management Procedure that details the standardised and agreed process for making changes to any of the people, process and/or technology components associated with the flow of data from source to target for the corporate collections for which they are responsible.

Essential aspects of the process include:

- All changes (whether planned and/or unplanned, as well as whether related to people, processes and/or technologies) should be managed in accordance with the agreed and standardised Change Management Procedure.
- Appropriate levels of authorisation are obtained before there is any significant investment made in implementing the change, which may include time, resources and funds.
- Approval to implement changes should be based upon comprehensive, detailed, accurate and reliable information regarding the following: business imperatives for the change; evaluation of the alternative options for responding to these imperatives; estimated effort in terms of time, resources and costs; and, assessment of associated risks.
- All stakeholders that are impacted by these changes should be kept informed of progress with their implementation.
- Clear approval pathways are defined for each of the levels of "criticality" regarding the request for change.
- The process map for the Change Management Procedure identifies the roles associated with the operational implementation of this process. It is recommended the MFTs assign these roles to appropriate members depending upon what stage in the dataflow process to which they contribute.

If, as part of your assessment of compliance with the 9 Directive Principles, a gap is identified whereby a change management procedure is needed, use of the additional guidance in the appendix is recommended. This will provide a baseline to work through as an MFT.

Technologies

This section is most appropriate for those business units where data management is a core business activity and responsibility..

Technology can be an effective enabler for executing procedures that have been standardised. It provides those responsible for implementing them with the ability to simplify complex tasks as well as automate repetitive tasks. This improves procedure execution by reducing time, costs and risk of human error.

The technologies that have been selected to support data quality management and improvement include:

South Australian Health Metadata Repository (SAHMR)

The South Australian Health Metadata Repository (SAHMR) is a centrally-managed register for storing, accessing and disseminating information regarding all health-related data standards. SAHMR is a "variant" of the Australian Institute of Health and Welfare's (AIHW) METeOR product that has been customised to meet the specific requirements of SA Health with respect to management of metadata.

Recommendations

MFTs for each of the corporate collections support and oversee the planning of a programme of work aimed at achieving the following objectives:

- Metadata describing each of the corporate collections is made available from the SAHMR and that it is confirmed as being accurate, complete and current.
- Where agreed and approved standards already exist for the data items held in these collections, they are published in SAHMR.
- When approved standards are not currently available and new standards need to be developed (in accordance with the Data Standards Development Procedure), SAHMR will be used to record progress in the development process that will conclude in the formal endorsement of a new data standard for SA Health via the ICT Standards Framework.

Providing ready access via online search through a single entry point to a centrally-managed repository of data standards authorised for use across SA health is an essential prerequisite for increasing awareness, knowledge and adoption of these standards for all corporate data collections across the whole enterprise. Hence, it is recommended that the MFT develop and implement strategies aimed at increasing awareness and use of SAHMR throughout their respective organisations. This will involve:

- Promotional activities aimed at raising awareness
- Providing training for staff that is required to use SAHMR, either in the management of existing standards, development of new standards and/or access to existing standards as required for implementing quality compliance checks.

Data Profiling

Data profiling is an essential component of a data quality management and improvement regime. It provides:

- Combination of automated discovery and interactive analysis for determining the nature and extent to which data complies with expectations (standards, rules)
- Complete understanding of data by identifying any inconsistencies, redundancies and inaccuracies
- Objective assessment, documentation and reporting of data that fails to comply with agreed quality criteria to inform subsequent decisions for data "cleansing" to rectify issues of non-compliance.

Recommendations

It is advised that MFTs consider the potential benefits to be gained from the use of data profiling technologies to help automate some of the quality compliance checking processes.

Options for implementing data profiling include:

- Static monitoring
  - Test data against expectations (pre-defined and agreed quality criteria).
  - Identify, document and notify relevant stakeholders where expectations are not met (non-compliance)
  - Initiate **Incident Management Procedure** to rectify the issue
  - Re-profile data periodically to confirm that the incident has been successfully rectified.
- Dynamic monitoring
  - Data profiling functions are embedded within the technologies that support the data flow and processing (e.g. data validation embedded in data entry screens; data checks embedded in existing ETL processes).
  - Check results of automated and dynamic data checks
  - Perform regular surveys of end users of the data to gather feedback on their assessment of data quality
  - Identify, document, notify stakeholders where data quality expectations are not being met.

Technical Metadata Management

Business metadata is information that is usually created primarily for business users to help them understand and interpret the data used to meet their business needs. *Technical* metadata is detailed information regarding the end-to-end processing of data from source through to final targets, including data structures, physical storage and any transformation processes. This information is generally used by the technical staff responsible for designing, building and/or maintaining the flows of data and its transformation.

Recommendations

It is recommended that technical metadata is documented for all information reporting systems that use corporate data and/or that support corporate business activities, including both primary and secondary uses.

When this technical metadata documentation does not already exist, it should be created using alternatives methods, such as using available technologies to automatically harvest this information directly from the data processing systems, including data sources, staging databases, data warehouses and final reports.

All technical metadata for key corporate collections should be published in the SAHMR that has been customised specifically for storing and displaying this information along with the corresponding business metadata.

Key technical metadata that should be captured and made available via SAHMR include:

- Use a common taxonomy of metadata definitions, along with their corresponding business names, to facilitate shared understanding and collaboration between the suppliers of information and their business clients
- Visual maps of data flows and dependencies across all systems and processes that illustrate the complete source-to-target lineage of data
- Ability to assess compliance to data quality standards at different data lineage points.
- Detailed dependencies between data assets to determine where they are used throughout a data integration solutions

- Audit trails for assessing the nature, extent and likelihood of any impacts of changes to data and/or systems, especially with respect to data quality compliance.

Utilising the tools and technology recommendations in areas of the business where 'data' is the core business will support and improve data quality management.

Competencies

Availability of a workforce with the appropriate competencies (levels of knowledge, experience, skills) is necessary to ensure successful execution of the standardised procedures and workflows that support good data quality management.

Recommendations

All staff contributing to and thereby responsible for managing data quality should be confirmed as possessing the minimum levels of competencies (knowledge, experience and skills) that are required for them execute their roles and responsibilities in accordance with pre-defined performance expectations. To achieve these objectives, organisations need to provide staff with access to appropriate competency-based training.

Steps involved in establishing a sustainable competency-based training capability include:

- Define the target audience for training.
  - Identify the different functional areas that contribute to data workflows and processing
  - Identify the staff responsible
  - Describe their work practices and workflows

- Determine & describe the competencies (levels of knowledge & skills) that would be required of each of the target groups to ensure that they are able to perform their data quality management responsibilities and met pre-defined performance expectations. These will include a working knowledge and understanding of:
  - Agreed quality standards that are relevant to the data being processed.
  - Expectations regarding the levels of compliance with these agreed quality standards.
  - Likely downstream business impacts of poor data quality for both primary & secondary uses of this data.
  - Need and ability to conduct regular data quality compliance checks to confirm that expectations regarding data quality compliance are met.
  - Established protocols and procedures for:
    - Conducting regular data quality compliance checks (Compliance Checking Procedure)
    - Notifying relevant parities of any incidents regarding non-compliance Incident Management Procedure)
    - Contributing to root-cause analyses aimed at diagnosing factors contributing to these incidents. (problem management procedure)
    - Contributing to activities aimed at resolving these data quality issues (change management procedure).

- Develop a local training capability that includes the following resources:
  - Training materials & resources
    - Instruction materials to be used during formal training sessions
    - Reference materials available online, such as information regarding the SA Health Metadata Repository (SAHMR) that provides online access to the data standards that are relevant to the corporate data collections.
    - User guides providing step-by-step instructions regarding implementation of the standard procedures for reporting incidents and/or root-cause analyses.
  - Training instructor

        - Identify resource(s) that is responsible for delivering current training to local staff or support to staff if eLearning training is available.
        - Provide local trainers with “train-the-trainer” instructions so that as well as being familiar with the course content, they have the skills to be effective trainers.

    - Training schedule
        - Develop a program of training sessions that will ensure all of the relevant staff receives the necessary training.

    - Evaluation
        - Design a method for assessing whether or not trainees have successfully met the minimum requirements regarding essential competencies.

5. Roles and Responsibilities

Data quality management is the responsibility of everyone within SA Health. Effective data quality management requires a whole-of-organisation approach with clear points of accountability at all levels of the organisation. Practical application of this Guideline should be appropriate to the significance of the data being managed and by the level of impact that poor quality of that data could have on the business.

Chief Executive – SA Health will:

- ensure the administration of data quality management across SA Health is in accordance with the Data Quality management Directives and associated Guideline

Chief Executive Officers for each LHN:

- will ensure sufficient resources are in place to enable the effective monitoring, recording and reporting of data quality, as well as investigation and implementation of recommendations for resolving data quality issues;
- will ensure the health units within their area of control have systems and processes in place to monitor data quality, investigate and implement the actions necessary to reduce the likelihood of incidents recurring, thereby improving delivery of clinical services and consumer safety;
- will ensure all identified data quality issues that have the potential to result in liability or have the potential to attract significant media attention are immediately escalated to the Chief Executive for SA Health, to Insurance Services and the Department’s claims manager; and
- may delegate the day-to-day responsibility for establishing and monitoring the implementation of this policy to relevant senior managers within their area of control.

Executive Directors, Directors, heads of service/ departments and other senior managers will:

- manage data quality within the areas of their control and ensure any corrective actions recommended as a result of investigation or review process are fully implemented and any subsequent impacts are closely monitored;
- develop, implement and monitor local processes to achieve effective data quality management, which should include training of relevant staff in data quality management processes and encourage an environment where reporting and active management of data quality is fostered; and
- ensure the effective management of data quality issues referred by front-line staff and managers.

Health Service Managers of Safety, Quality and Risk/Clinical Governance will:

- promote the Data Quality Management Directive and accompanying Guideline;
- assist others to ensure that the health unit/region meets its obligations under this Directive and guideline; and,
- provide support and advice to staff managing data quality issues.
- Adhere to risk management framework for identifying and managing risks associated with data quality as specified by the SA Health Risk Management Framework

Health Service Managers / Supervisors will:

- ensure that all data quality issues that they become aware of are addressed and successfully resolved within appropriate timeframes; and
- effectively manage these issues in accordance with this SA Health Data Quality Management Guideline.

All SA Health employees or persons will:

- adhere to the principles and aims of this policy and ensure they operate in accordance with its associated guidelines and procedures.

Note: A role based responsibility matrix has been provided in appendix E.

6. Reporting

N/A

7. EPAS

N/A

8. National Safety and Quality Health Service Standards

National Standard 1 Governance for Safety and Quality in Health Care	National Standard 2 Partnering with Consumers	National Standard 3 Preventing & Controlling Healthcare associated infections	National Standard 4 Medication Safety	National Standard 5 Patient Identification & Procedure Matching	National Standard 6 Clinical Handover	National Standard 7 Blood and Blood Products	National Standard 8 Preventing & Managing Pressure Injuries	National Standard 9 Recognising & Responding to Clinical Deterioration	National Standard 10 Preventing Falls & Harm from Falls
☒	☐	☐	☐	☐	☐	☐	☐	☐	☐

9. Summary

These guidelines provide information regarding each of the following DQMF components as well as advice regarding their establishment and operational implementation:

- **Guiding Principles:** Linked into the data quality Directives - appropriate to all SA Health employees.
- **Organisational Governance:** Recommended approach using MFTs to get the right people around the table to agree roles and responsibilities for managing data quality - appropriate to all SA Health employees.
- **Policies:** DQMF documentation including Directives - appropriate to all SA Health employees.
- **Standards:**
    - **Data:** Standardised definitions and requirements - predominantly appropriate to those with 'data' as their core business.
    - **Process:** Standardised ways of working:
        - Data Standards Development - predominantly appropriate to those with 'data' as their core business.
        - Compliance, Change, Problem & Incident Management - appropriate to all SA Health employees.
- **Technologies:** Identified tools and technologies to support data quality management– predominantly appropriate to those where data is a core business activity and responsibility.
- **Competencies:** Key knowledge and understanding of data quality impact across the business – appropriate to all SA Health employees.

There is extra information in the appendix about the DQMF as well as examples of recommended standardised procedures, recommended membership, roles and responsibilities of the MFTs, and a data quality assessment check list. These documents provide additional support if your area needs to address one or more of the DQMF areas to comply with the Data Quality Directives.

10. Risk Management

It is important to be aware of risks resulting from non-compliance with the DQMF directives such as the inability to provide all users across the enterprise with access to information that is quality-assured for meeting their specific business requirements. The guiding principles have been designed to establish an appropriate control environment to manage data quality related risks so that the overall residual risk level is reduced from the initial, uncontrolled total risk. Application of these controls at an operational, tactical and strategic level in accordance with the SA Health Risk Management Framework will enable SA Health to manage its data quality risks in an appropriate manner.

11. Evaluation

N/A

12. Definitions

In the context of this document:

- **Change Management Procedure** means:

Formalised and standardised steps for managing changes (both planned and/or unplanned) to data, processes and/or systems that are designed to ensure that their implementation results in minimal disruptions to the business they support.

- **Compliance Checking Procedure** means:

Formalised and standardised steps for regular profiling of data to check compliance with pre-defined and agreed quality assessment criteria, where findings provide basis for confirming that the data is "fit-for-purpose" and if not, then triggering an Incident Management Procedure.

- **Corporate Performance Management Reporting Framework** means:

Information architecture designed to ensure that the same transactional data collected in local operational systems is used to meet the performance management reporting requirements at each of the levels of management, commencing at the local health unit, regional metropolitan LHN and/or country Hospital Cluster, eventually for the whole enterprise.

- **Data Custodian** means:

Responsibility for managing the data collections that support specific reporting requirements.

- **Data entry** means:

Initial capture of data that is entered into local operational systems, as well as any subsequent updates to this data, by authorised staff including both administrative and medical.

- **Data Quality Management Framework** means:

Set of agreed standards regarding data, processes, technologies, workforce competencies and governance arrangements that need to be adopted consistently across the enterprise if the organisational strategic objectives regarding improvements in corporate data quality are to be achieved.

- **data monitoring** means:

Regular re-profiling of data to check its compliance with agreed data quality assessment criteria and to retain a history of improvements in data quality over time following the establishment and operational implementation of the Data Quality Management Framework.

- **data profiling** means:

Quantitative measurement and assessment of data compliance with agreed pre-defined quality criteria.

- **Data Provider** means:

Responsibility for ensuring that the data available within operational systems that are the data sources for corporate collections meets all of the agreed quality assessment criteria and thereby confirmed as being "fit-for-purpose" with respect to both primary and secondary uses of this data.

- **Data Standards Development Procedure** means:

Formalised and standardised steps for the development of new and/or amendments to existing data standards.

- **Data submission** means:

Data from local operational systems is used to create an extract that is then submitted to the Data Custodians within the Funding and Performance Evaluation branch that are responsible for managing data quality for each of the corporate collections.

- **Incident Management Procedure** means:

Formalised and standardised steps for rectifying any incidents where data is found not to comply with expected quality targets as soon as possible to minimise risk of disruptions to downstream business activities that use the data.

- **ICT infrastructure** means:

The technologies, including the hardware and software, that collectively provide the technical environment that supports the end-to-end flows and processing of data from source through to final targets.

- **ICT Standard Framework** means:

Formalised and standardised protocols and procedures for managing ICT standards across SA Health, which includes the mechanisms for the development and endorsement of new standards.

- **METeOR** means:

The repository for national metadata standards for the health, community and housing assistance sectors across Australia developed by the Australian Institute of Health and Welfare to serve as a registry for storing, managing and disseminating metadata based upon the international standard ISO/TEC 11179 for metadata.

- **primary use** means:

Principal reason for data collection and use.

- **Problem Management Procedure**

Formalised and standardised steps for rectifying any problems regarding repeated failure of data to comply with expected quality targets as soon as possible to minimise risk of disruptions to downstream business activities that use the data.

- **SA Health Metadata Repository (SAHMR)** means:

The local version of METeOR that has been customised to meet the specific needs of the SA Health with regards to storage, management and dissemination of metadata regarding corporate collections.

- **secondary use** means:

The use of transactional data collected in local operational systems to meet business reporting requirements beyond those for which the data was initially collected (i.e. primary use).

13. Associated Policy Directives / Policy Guidelines

- Data Quality Management Directive
- SA Health Risk Management Framework

14. References, Resources and Related Documents

The following documents are referenced in this document:

- Data Quality Compliance Checking and Certification Procedure for New ISAAC
- ICT Governance Framework
- ICT Standards Framework
- Information Classification and Management Specification
- Data Quality Management Directive

- METeOR (http://meteor.aihw.gov.au/content/index.phtml/itemId/181162)
- National Data Dictionaries (http://www.aihw.gov.au/datadevelopment/data_standards/data_dictionaries.cfm)
- National Health Data Dictionary (http://www.aihw.gov.au/publications/index.cfm/title/10049)
- National Health Information Model (http://www.aihw.gov.au/publications/index.cfm/title/8821)
- National Health Information Management Group (NHIMG)
- National Community Services Information Management Group (NCSIMG) http://www.aihw.gov.au/ncsimg/
- Participation Data Specification version 3.0 - 25 August 2010 (http://www.nehta.gov.au/component/docman/doc_download/1122-participation-data-specification-v30)
- South Australian Cancer Registry Notification Manual.

The following documents are related to this policy:

- Data Quality Management Directives
- Data Standards Development Procedure
- Compliance Checking Procedure
- Incident Management Procedure
- Establish a problem management procedure
- Establish a change management procedure
- SA Health Risk Management Framework