Policy

Policy Directive: compliance is mandatory

Data Quality Management Policy Directive

Objective file number: 2011-12910, eA517459
Document classification: For Official Use Only-I2-A1
Document 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 Policy Directive is to achieve enterprise-wide adherence to the set of standards regarding data, processes, technologies and workforce competencies that are required to deliver the organisation’s strategic objectives regarding continuous data quality improvement.
Keywords	Data quality management framework, data quality management data standards, data governance, Data Quality Management Policy Directive
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 impacted	*All Staff, Management, Admin, Students; Volunteers*
EPAS compatible	*Yes*
Registered with Divisional Policy Contact Officer	*Yes*
Policy doc reference no.	D0266

Version control and change history

Version	Date from	Date to	Amendment
1.0	16/02/2012	09/04/2015	Original version endorsed by PE
1.1	09/04/2015	Current	Reviewed and updated Risk Management sections

Government
of South Australia

SA Health

Data Quality Management Policy Directive

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
Anticipated Date of Review	30 April 2018

Document history

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

Contents Page

1. Objective 4
2. Scope 4
3. Principles....5
4. Detail 9
5. Roles and Responsibilities....13
6. Reporting....14
7. EPAS....14
8. Exemption 14
    8.1 Exemption Scope....14
    8.2 Exemption Process....14
9. National Safety and Quality Health Service Standards 14
10. Risk Management 14
11. Evaluation 15
12. Definitions 15
13. Associated Policy Directives / Policy Guidelines 16
14. References, Resources and Related Documents....16

Data Quality Management Policy Directive

1. Objective

The purpose of this document is to define the 9 key ‘guiding principles’ that provide clear expectations regarding adherence to standards for data, processes, technologies, competencies and governance that will be required to achieve the organisation’s strategic objectives regarding continuous improvement in data quality. It should be read in conjunction with the supporting Data Quality Management Guidelines document that provides the recommended ‘best practices’ for application of data quality management across the business and also explains in more detail the DQMF elements.

2. Scope

The scope of this Directive 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 Networks and SA Ambulance Service – The same data is also used to support **tactical** decisions such as at optimising the use of available resources across multiple sites within a region to make best use of available capacity.
- SA Health – The same data is used to support a wide range of **strategic** decision making regarding policy, performance, funding and planning that requires data collected from across organisational boundaries to be aggregated to create an enterprise-wide view.

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

(b) All elements of the *Data Quality Management Framework* illustrated in figure 1 and Appendix A.

(c) Application of the *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 information reporting systems, whereby it becomes embedded within the current data management activities across SA Health.
- **New data and/or application development** – 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 Systems for all new ICT system development.

3. Principles

The following ‘principles’ will deliver upon the strategic objective of improving the quality of information available to support better business decisions. Directives are the mechanisms for translating the guiding principles for improving the quality of corporate data into pragmatic, actionable and measurable strategic objectives for the organisation. They direct the formal development of agreed standards (for both data and processes) and their subsequent adoption across the enterprise, as both are required to achieve these strategic data quality management objectives.

Directive Principle 1: Data quality will be managed with the diligence of other strategic corporate assets.
Data supports most core business functions and activities for different business units across the enterprise, at all levels of organisational management. 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 that will require the following:

- Senior executive sponsorship and support for organisational data quality management initiatives.

- Leveraging, where appropriate, existing corporate governance structures and processes already established to support the strategic objective of ICT infrastructure standardisation across the SA Health enterprise, given the close similarity with the data quality management objectives in terms of data and process standardisation.

- Regular monitoring, measurement, assessment and reporting of the level of data compliance against relevant and agreed quality targets to embed an ongoing discipline of standardisation, ownership and accountability for managing data aimed at improving the quality of information available to better support the organisation’s business activities.

Directive Principle 2: Data quality management is an enterprise-wide responsibility.
The processing of data from the point of initial capture through to final reporting involves contributions from many individuals that depend upon their collaboration and cooperation across organisational boundaries. Quality behaviours of data collectors, processors, custodians and analysts can 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.

Since data quality issues can arise at any stage in the processing of data and impact upon downstream processes, all contributors have a shared and collective responsibility in managing data quality. This will require:

- Clear stewardship for data being established within operational business units whereby they are accountable for confirming that the data they provide to support both local and enterprise-wide reporting complies with the agreed enterprise-wide and appropriate quality assessment criteria.

- Staff having access to relevant competency-based training to acquire the skills necessary to perform these functions in accordance with the agreed standards and performance expectations.

- All data users, including producers and consumers, to be educated on data quality objectives and standards as well as being provided with the context of how the quality of their work impacts the business.

- Data quality initiatives must have adequate business resources to provide context and insight into potential data quality problems.

Directive Principle 3: Data will be common across the enterprise with regards to definitions, interpretations, formats and/or business rules for any derived data, unless there is an accepted and documented business justification for deviation.
Compliance with agreed standards will promote consistency in the meaning and interpretation of data wherever it is available across the enterprise. Achieving consistency in data used across the enterprise will require the following:

- Standards need to be established for all key corporate data and they need to be adopted for all key corporate collections.

- Existing standards are to be adopted, where they already exist and where they are appropriate, in the following descending order of priority: national; state; inter-state or international.

- When existing standards are not available, local standards should be developed using the recommended Data Standards Development Procedure that utilises, where appropriate, the procedures and governance arrangements that have already been established under the existing ICT Standards Framework and ICT Governance Framework.

- Variations to the above recommendations require approved exemption via an agreed exemption process.

- Where different collections using data from the same sources require different standards 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.

Directive 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 repository that is centrally-managed as the authoritative source. Providing ready access to an authoritative source of information regarding data standards will require the following:

- Existing SA Health Metadata Repository (SAHMR) is endorsed as the single repository for storing metadata for corporate data and collections, especially the data standards that are managed by the Data and reporting Services Branch.

- Data custodians responsible for managing the key corporate collections are required to ensure that the metadata available within SAHMR related to their corporate collections is complete, accurate, reliable and current.

- A recognised central metadata repository appropriate to the business area should be utilised and should provide links to an agreed central repository suite (including SAHMR).

- Data standards available within a recognised central metadata repository should be the criteria used for all data quality checks in accordance with the recommended data quality Compliance Checking Procedure.

Directive Principle 5: All data must be referenced to a single source of truth
To ensure consistency in information reporting across the organisation, regardless of the reporting system used, it should be from the one authorised “source-of-the-truth”. This requirement applies equally to data used to meet local “primary-use” requirements as well to data that is used to meet enterprise-wide “secondary-use” reporting requirements. For all reporting to be based upon the same data source, the following is required:

- Wherever possible, transaction data entered into local operational systems should be the source of data used for reporting at all levels of organisational management. This is represented as a cascade of information reporting requirements starting with unit record transactional data to support local operational activities being progressively aggregated and summarised to provide an enterprise-wide view of the data to support tactical and strategic decision making (Appendix B: Corporate Performance Management Reporting Framework).

- Data required for secondary-use reporting should be extracted from local operational systems at the level of unit record, which is subsequently aggregated and/or summarised as required by the different levels of reporting. The data flow and information architecture for all reporting systems should be traceable back to the unit record level data.

- Data Providers are required to confirm that the data available within local operational systems is confirmed as meeting agreed data quality assessment criteria and targets.

Directive Principle 6: Standards need to be established for the execution of data quality management processes and work practices.
Standardised protocols and procedures need to be established and enforced to ensure the efficient and effective execution of good data quality management processes, especially those associated with the regular monitoring of compliance with agreed quality targets, as well as the resolution of any data quality issues detected. To ensure the efficient and effective execution of good data quality management practices, the following protocols and baseline procedures are recommended for consistent adoption:

- Data Standards Development Procedure 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 will align with the existing ICT Standards Framework and ICT Governance Framework.

- Compliance Checking Procedure for the regular measurement, monitoring, evaluation and reporting of compliance against pre-defined and agreed data quality criteria, with the findings subsequently providing the basis for confirming whether or not they have been met.

- Incident Management Procedure for managing incidents, which are defined as any “event” that has or may have the potential to negatively impact on data quality compliance and result in disruptions to the business activities supported by this data. The aim is to rectify them as soon as possible to minimise any risks of disruptions to the business.

- Establishment of a Problem Management Procedure, 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.

- Establishment of a Change Management Procedure 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.

Directive Principle 7: Address data quality issues "upstream" as close as possible to the point of initial data capture and entry into operational systems.
Principle source of poor data quality is at the initial point of data capture, especially when it is entered manually into operational systems. Hence, data quality problems are best addressed as close as possible to the initial point of data entry. Effective and efficient mechanisms for mitigating the risks of poor quality data being entered into operational systems include the following:

- All staff authorised to enter and/or update data in local operational systems are trained and have the necessary levels of competencies (knowledge and skills) that are required for data entry.

- Where possible, appropriate data quality technologies are integrated and embedded within the operational system application. These technologies would include:

  - Real-time validation of data as it is entered. Common application of these technologies is the validation of address data whereby the system automatically alerts the data entry operators when the address data typed into the data entry fields does not match with the authorised lists of addresses. This permits the data entry operator to re-type the correct address before it is entered into the operational system.

  - Other data quality technologies include reducing the opportunities for free text entry by requiring data entry operators to select from a prescribed list of approved data values.

Directive Principle 8: Profile data frequently, broadly, collaboratively and transparently.
To effectively manage data quality, efforts must be made to proactively monitor the data environment at each step in the dataflow process. This will require the incorporation of the following practices as part of the regular data management activities:

- Data profiling – Regular measurement, assessment and reporting of data compliance with required quality criteria that provides all stakeholders with information regarding data quality status that is accurate, reliable and up-to-date.

- Data monitoring - Regular re-profiling of data to create 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.

Note:

- All data profiling and/or monitoring that is associated with data quality compliance auditing will be based upon the relevant data standards published in the metadata repository.

- Any "cleansing" of data to rectify quality issues that have been detected during compliance auditing will be based upon pre-defined and agreed enterprise-wide data definitions and business rules.

Directive 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, the following are required:

- 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.

4. Detail

Achieving the organisation's strategic objectives regarding improvements in data quality requires adherence to a set of standards around data, processes, technologies, skills and governance for managing data with continuous improvement the goal. Collectively, this set of standards provides a framework (*Data Quality Management Framework*) for managing the quality of data at each step in the complete end-to-end flow and processing of data from its initial point of capture in source systems through to final outputs. Compliance with these standards will enable the delivery of information to all users across the enterprise that has been assessed and confirmed as meeting agreed data quality criteria and thereby "fit-for-purpose" in meeting their business requirements. It serves to embed an ongoing discipline of standardisation, ownership and accountability for managing data quality as part of the regular data management activities associated with all corporate data.

A *Data Quality Management Framework* (DQMF) includes the following elements (see Figure 1):

- **Guiding Principles:** Statements regarding foundational capabilities required to achieve high-level objectives with respect to excellence in 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 quality management, including data definitions, quantitative metrics for assessing data quality, as well as performance in executing the processes that provide procedural direction over the logical sequence of tasks to achieve and measure compliance with the standards and policies set out by the organisation.
- **Technologies:** "Tools" that enable execution and compliance measurement of data quality management policies, standards and processes.
- **Competencies:** Workforce skills 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 all decision rights and accountabilities regarding data quality management.

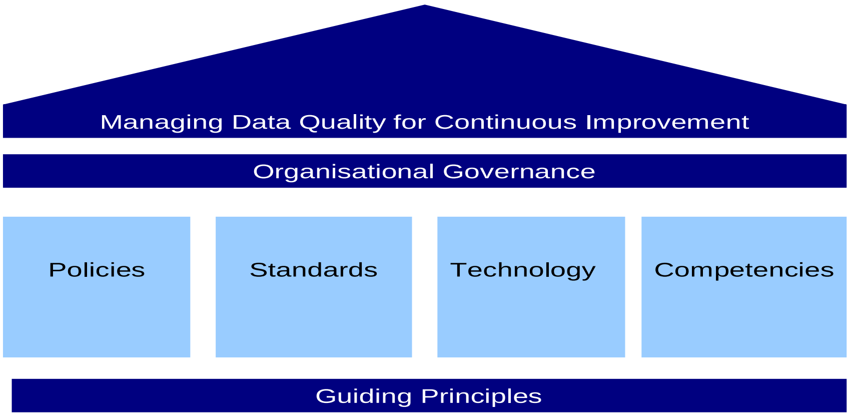
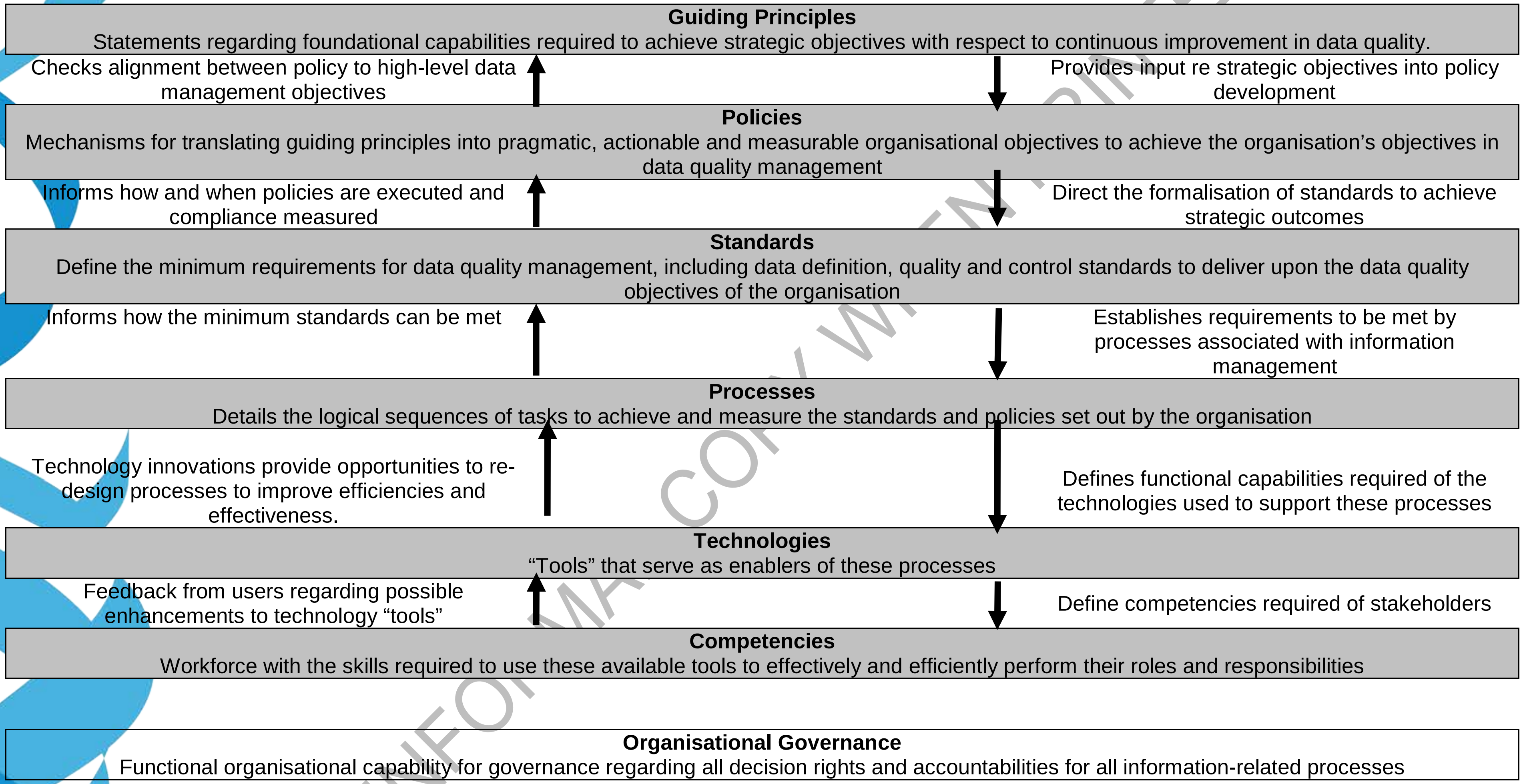

Managing Data Quality for Continuous Improvement
Organisational Governance
Policies
Standards
Technology
Competencies
Guiding Principles

Figure 1: Data Quality Management Framework (DQMF) elements

To support the business in meeting its health reform agenda responsibilities, SA Health will utilise a DQMF. Implementation of the DQMF will provide direction and structure to enable SA Health to effectively manage and govern data quality and imbed key quality principles into everyday processes.

Cascading dependencies between elements in SA Data Quality Management Framework



Guiding Principles

Statements regarding foundational capabilities required to achieve strategic objectives with respect to continuous improvement in data quality.

Checks alignment between policy to high-level data management objectives

Provides input re strategic objectives into policy development

Policies

Mechanisms for translating guiding principles into pragmatic, actionable and measurable organisational objectives to achieve the organisation's objectives in data quality management

Informs how and when policies are executed and compliance measured

Direct the formalisation of standards to achieve strategic outcomes

Standards

Define the minimum requirements for data quality management, including data definition, quality and control standards to deliver upon the data quality objectives of the organisation

Informs how the minimum standards can be met

Establishes requirements to be met by processes associated with information management

Processes

Details the logical sequences of tasks to achieve and measure the standards and policies set out by the organisation

Technology innovations provide opportunities to re-design processes to improve efficiencies and effectiveness.

Defines functional capabilities required of the technologies used to support these processes

Technologies

"Tools" that serve as enablers of these processes

Feedback from users regarding possible enhancements to technology "tools"

Define competencies required of stakeholders

Competencies

Workforce with the skills required to use these available tools to effectively and efficiently perform their roles and responsibilities

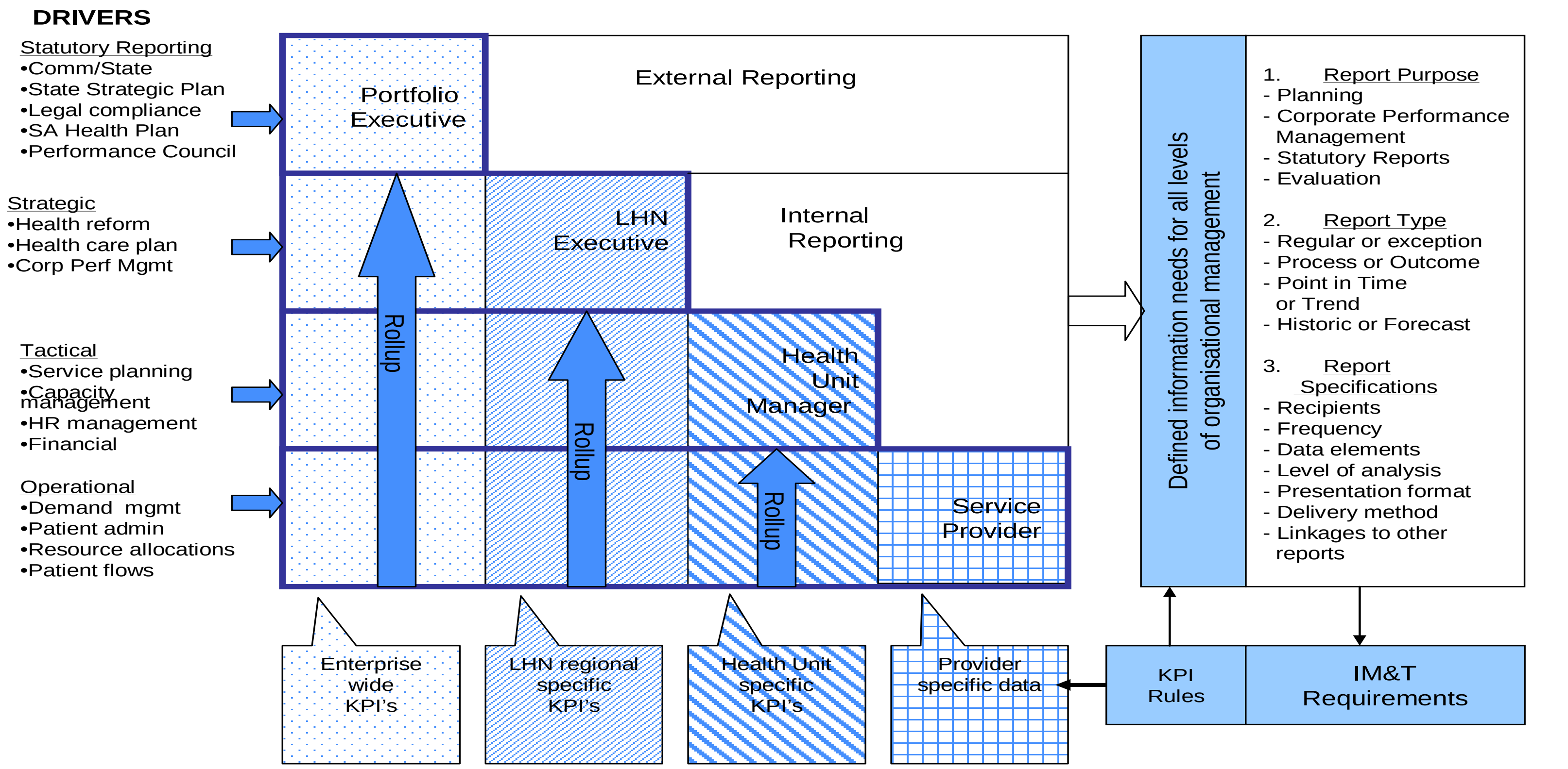
Organisational Governance

Functional organisational capability for governance regarding all decision rights and accountabilities for all information-related processes

Corporate Performance Management Reporting Framework

Corporate Performance Management Reporting Framework

"CPM reporting at all levels of management is based on data collected as by-product of service delivery"



DRIVERS

Statutory Reporting
- Comm/State
- State Strategic Plan
- Legal compliance
- SA Health Plan
- Performance Council

Strategic
- Health reform
- Health care plan
- Corp Perf Mgmt

Tactical
- Service planning
- Capacity management
- HR management
- Financial

Operational
- Demand mgmt
- Patient admin
- Resource allocations
- Patient flows

Portfolio Executive

External Reporting

LHN Executive

Internal Reporting

Health Unit Manager

Service Provider

Rollup

Rollup

Rollup

Enterprise wide KPI's

LHN regional specific KPI's

Health Unit specific KPI's

Provider specific data

Defined information needs for all levels of organisational management

1. Report Purpose
- Planning
- Corporate Performance Management
- Statutory Reports
- Evaluation

2. Report Type
- Regular or exception
- Process or Outcome
- Point in Time or Trend
- Historic or Forecast

3. Report Specifications
- Recipients
- Frequency
- Data elements
- Level of analysis
- Presentation format
- Delivery method
- Linkages to other reports

KPI Rules

IM&T Requirements

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 for monitoring and reporting feedback at all levels of the organisation. Practical application of the directives 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 this policy

Chief Executive Officers - Local Health Network (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 related to poor data quality recurring, thus 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 of 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 that the recommended corrective actions resulting from the investigation or review process are fully implemented and monitored;
- develop, implement and monitor local processes that support employees and other persons providing health services on behalf of SA Health to achieve effective data quality management. This should include training 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 this data quality management policy and accompanying guidelines;
- assist others to ensure that the health unit/region meets its obligations under this policy; 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 the SA Health Data Quality Management Guideline.

All SA Health employees or persons who provide health services on behalf of SA Health will:

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

6. Reporting

N/A

7. EPAS

N/A

8. Exemption

8.1 Exemption Scope

No exemption allowed for this policy directive

8.2 Exemption Process

No exemption allowed for this policy directive

9. 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
☒	☐	☐	☐	☐	☐	☐	☐	☐	☐

10. Risk Management

It is important to be aware of risks resulting from non-compliance with these 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 the 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 CHSA 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 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

The following documents are related to this policy:

- Data Quality Management Guidelines
- ICT Governance Framework
- ICT Standards Framework
- SA Health Risk Management Framework

14. References, Resources and Related Documents

The following documents are referenced in this document:
METeOR (http://meteor.aihw.gov.au/content/index.phtml/itemId/181162)
Code of Fair Information Practice
Information Classification and Management Specification

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