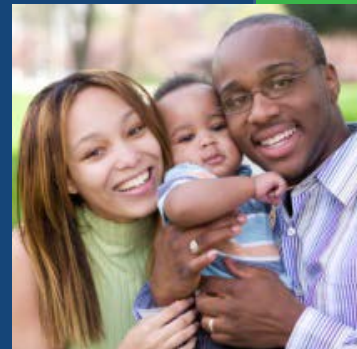

Framework Subcomponent: Data Governance and Management

Excerpt from *DaSy data systems framework* by The DaSy Center (Menlo Park, CA: SRI International, 2014), 11-16.

September 2014



Subcomponent: Data Governance and Management (DG)

Data governance is both an organizational process and a structure. Data governance establishes responsibility for data, organizing program staff to collaboratively and continuously improve data quality through the systematic creation and enforcement of policies, roles, responsibilities, and procedures. Management is the systematic development, implementation, and enforcement of procedures (standardization of business processes) to operationalize the quality and security policies of the data system. Management addresses the implementation of data governance policies (via procedures) and oversees the operations of the data system.

Data governance exists whether formal or informal. Informal data governance is associated with significant risks. These risks may include:

- Questionable data quality, security, and usefulness of data
- Difficulty in maintaining consistent and reliable data and processes
- Unclear roles and responsibilities of internal and external staff relative to the data
- Inappropriate data sharing within internal and external staff and across external agencies

Formal data governance has significant benefits. These benefits include:

- Increased likelihood that data are of high quality and protected
- Increased use of data in ways consistent with the purpose and vision of the data system
- Increased confidence in data and associated processes (e.g., oversight of analysis activities)
- Improved fiscal efficiency and accountability

Data governance structures and policies are not static; they must evolve as the programs and policies that drive the data systems evolve. Managing the state data system requires responding to the evolving structures and policies and implementing the associated procedures. Part C and Section 619 state staff or their representatives should be actively engaged in the governance of their data system. This subcomponent uses the phrase “data governance structure.” A data governance structure is the formalized entities or individuals charged to establish policy and procedures for the overall management of the data and data system. In some states, there may be more than one data governance structure. The indicators and elements apply to all structures in a state.

This subcomponent consists of three sections. The first section, authority and accountability, is about establishing the data governance and management structure(s), responsibility, and oversight. The second section, quality and integrity, addresses policies to ensure validity, reliability, accuracy, consistency, and intended use of data. The section also focuses on the implementation of the monitoring and training procedures to ensure consistent application of data quality and integrity policies. The third section, security and access, focuses on the protection of state data from loss, contamination, or unintended uses and ensuring appropriate access.

Section 1: Authority and Accountability

Quality Indicator DG1: The data governance structure delineates appropriate decision-making authority and accountability consistent with the uses of the data system reflected in the purpose and vision.

Elements of Quality
DG1a. State-level, formalized data governance structure is authorized or assigned to make decisions about the Part C/619 data system.
DG1b. The data governance structure includes representatives from Part C/619 state programs who have decision-making authority.
DG1c. The data governance structure oversees all data collected and maintained by Part C/619 and ensures adherence to governance policies related to Part C/619 data, regardless of where the data are located.
DG1d. The data governance structure’s authority is reviewed and revised as necessary.

Quality Indicator DG2: The state ensures data governance and management roles and responsibilities clearly establish decision-making authority and accountability.

Elements of Quality
DG2a. A written statement(s) (e.g., organizational chart, data sharing agreements) delineates decision-making authority for Part C/619 data decisions.
DG2b. All data-related responsibilities associated with the Part C/619 state data system(s) are clearly assigned to responsible and informed parties (e.g., data manager, data steward, data owner).
DG2c. Information about data governance decision-making authority is communicated to staff and stakeholders (e.g., dissemination of organizational chart, policies and data sharing agreements).
DG2d. Data governance policies are developed with input from stakeholders and vendors and are reviewed and revised as necessary.
DG2e. Data governance policies address Part C/619 representation on other data governance structures and describe the extent of their decision-making authority as it relates to Part C/619 state data.

Quality Indicator DG3: Data governance authorizes Part C/619 staff or representatives to implement policies established for the state Part C/619 data system and manage the data system in accordance with all policies.

Elements of Quality
DG3a. A process is in place to allow Part C/619 staff or representatives to recommend policy changes to the data governance structure via their Part C/619 data governance representative.
DG3b. All requirements (e.g., operational, research, reporting) for Part C/619 data are clearly defined to ensure oversight and accountability.
DG3c. Part C/619 staff or representatives approve, prior to implementation, plans for substantive Part C/619 data system changes proposed by information technology (IT) (e.g., enhancements, business rules, technology changes).
DG3d. Part C/619 staff or representatives review and revise the state data system's operating procedures to be responsive to changes in state and federal policy (e.g., new or revised data collection standard to meet reporting requirements).
DG3e. Part C/619 staff or representatives communicate the state data system's operating procedures to staff and stakeholders.

Section 2: Quality and Integrity

Quality Indicator DG4: Data governance policies require the development and implementation of procedures to ensure the quality and integrity of data collected from state/local programs and agencies.

Elements of Quality
DG4a. Data governance policies require that data included in the state data system are aligned with the purpose and vision of the Part C/619 data system.
DG4b. Data governance policies require procedures to ensure the validity of Part C/619 data.
DG4c. Data governance policies require a point of contact for each state Part C/619 data transfer or exchange.
DG4d. Data governance policies require the development of data quality and integrity procedures for the state data system.
DG4e. Data governance policies require staff and contractors who collect, maintain, and/or receive state data to participate in ongoing data quality and integrity training.
DG4f. Data governance policies related to data quality and integrity of the state data system are regularly reviewed and adjustments are made as necessary.
DG4g. Data governance policies require that any internal or external program or agency maintaining and/or using state Part C/619 data adhere to applicable data quality policies and procedures.
DG4h. Data governance policies require that supporting documentation is available to ensure interoperability when transferring state Part C/619 data to other programs or agencies (e.g., data dictionaries, data validation checks).

Quality Indicator DG5: Part C/619 state staff or representatives implement monitoring procedures and technical assistance to ensure consistent application of data quality and integrity policies.

Elements of Quality
DG5a. Part C/619 state staff or representatives communicate to data system users regularly about Part C/619 data quality and integrity policies and procedures.
DG5b. Part C/619 state staff or representatives monitor the implementation of the data quality and integrity procedures for Part C/619 data.
DG5c. Part C/619 state staff or representatives have a data quality orientation training for data managers at the state and local levels.
DG5d. Part C/619 state staff or representatives create and maintain standardized training materials regarding procedures and responsibility for Part C/619 data system quality and integrity operations.
DG5e. Part C/619 state staff or representatives ensure adherence to data quality and integrity procedures when Part C/619 data are exchanged or transferred.
DG5f. The Part C/619 data system's data quality procedures are reviewed and revised periodically and as new management needs arise (e.g., establishment of memorandum of understanding [MOU] with other existing early childhood data system or external research requests).

Section 3: Security and Access

Quality Indicator DG6: Data governance policies require the development and implementation of procedures to ensure the security of the data from breach or loss.

Elements of Quality
DG6a. Data governance security policies are in place and available to Part C/619 state staff.
DG6b. Data governance security policies adhere to all federal, state, and local laws, regulations, and standards.
DG6c. Data governance security policies apply to all Part C/619 data collected, maintained, and/or used.
<p>DG6d. Data governance security policies require documenting data system operations which, at a minimum, include the following for each state data system:</p> <ul style="list-style-type: none"> • Person(s) responsible for data security • Data training for authorized data users • Data storage method • Data back-up and recovery • Response to data breach • Data transference (e.g., agency to agency, email, FTP, texting, USB) • Data encryption • Data destruction • Employee use of program equipment and personal devices
DG6e. Data governance security policies require that staff and contractors who collect, maintain, or receive data participate in periodic training about data security.
DG6f. Data governance security policies require adherence to security policies and procedures when transferring or exchanging Part C/619 state data.
DG6g. Data governance security policies require that all internal or external entity or agency maintaining or using state Part C/619 data adhere to all applicable security policies and procedures.
DG6h. Data governance security policies are periodically reviewed and revised as necessary.

Quality Indicator DG7: Data governance policies require the development and implementation of procedures to ensure that only authorized users gain appropriate access to the data, including reports.

Elements of Quality
DG7a. Data governance access policies are in place and available to all state Part C/619 state staff.
DG7b. Data governance access policies adhere to all federal, state, and local laws, regulations, and standards.
DG7c. Data governance access policies apply to all Part C/619 data collected, maintained, and/or used.
DG7d. Data governance access policies require that internal (and, to the extent required, external) Part C/619 data users participate in relevant access trainings regarding Part C/619 data.
DG7e. Data governance access policies require Part C/619 state staff or representatives to routinely monitor and test data system access to ensure effective and consistent implementation.
DG7f. Data governance access policies are periodically reviewed and revised as necessary.

Quality Indicator DG8: Part C/619 state staff or representatives support and implement management procedures that maintain and address data security and access.

Elements of Quality
DG8a. Part C/619 state staff or representatives communicate regularly to data system users about Part C/619 data security and access policies, and procedures.
DG8b. Part C/619 state staff or representatives monitor the implementation of the security procedures and the overall security of Part C/619 data.
DG8c. Part C/619 state staff or representatives monitor to ensure that all data users, at all levels, with access to state Part C/619 data adhere to the policies and procedures.
DG8d. Part C/619 state staff or representatives monitor to ensure adherence to security procedures when transferring or exchanging Part C/619 state data.
DG8e. Part C/619 state staff or representatives develop training materials regarding procedures and responsibility for Part C/619 data system security and access operations and data use.
DG8f. Part C/619 state staff or representatives require that all individuals with access to Part C/619 data demonstrate knowledge about security and access policies and procedures.
DG8g. Part C/619 state staff and representatives review and revise security and access training materials periodically and as new management needs arise (e.g., new or revised data policies).
DG8h. Part C/619 state staff and representatives review and revise procedures for monitoring security and access as necessary.