ALABAMA MEDICAID AGENCY INTERNAL MEMORANDUM NO. 918
DATE: May 1, 2020
SUBJECT: Data Governance

BACKGROUND

Management of Medicaid's data assets is a necessary component of ensuring the availability of and access to appropriate health care for all Medicaid-eligible Alabamians. Medicaid protects its data assets through security measures that ensure the proper access to and use of data. The security measures comply with appropriate federal and state regulations and requirements for privacy, protection, and confidentiality.

To manage this critical responsibility, Medicaid, through the Data Governance Charter, has established the position of Chief Data Officer ("CDO") and vests the CDO with the authority and responsibility to develop, implement, and manage Medicaid's Enterprise Data Governance Initiative through the Data Governance Office ("DGO").

Establishing Enterprise Data Governance ("EDG") is a critical task for Medicaid. It requires defining the organizational vision, policies, and practices, gaining the support of stakeholders, implementing the initiative, and monitoring its success. Initiation of external entity request for data shall initiate through DGO. The Data Governance Charter outlines policies, standard procedures, responsibilities, and controls surrounding data activities.

POLICY

The DGO has established the following policies to meet the objectives of the Medicaid Enterprise Data Governance Program:

1. **Data Management Policy**
   a. Policy
      i. The DGO, which serves as the Compliance Office for Data Governance, and Data Governance Council (DGC), comprised of Medicaid's Executive Staff, shall have the overall responsibility for the management and governance of Medicaid data.
      ii. The DGC shall be the authority and approving steward for defining, encouraging the utilization of, and for resolving conflicts in data management.
      iii. The DGO, in conjunction with the Data Governance Committee (DGCM), comprised of Medicaid's data and/or functional process owners shall develop data management practices. Processes that support these techniques may align with industry best practices while complying with Federal, State, and Local information security policies and privacy regulations.
      iv. The DGO shall develop a Data Stewardship program to assign ownership to Medicaid's data assets and establish a network of stewards and custodians to define and execute data management processes. Medicaid data shall be managed by domain, with data resource and/or functional process owners, and data steward(s)/manager(s)/custodians assigned to each data domain.

v. Prior to implementation, any new or modified data management methods shall be reviewed by the DGCM prior to their submission to the DGC for approval.

2. Data Quality Policy

The primary objective of the Data Quality policy is to ensure that Medicaid's data retains value and is useful for its intended purpose. The policy, through active monitoring, maintenance, and reporting, enables the DGO and supporting infrastructure to identify and react to data quality issues in a more timely fashion. The goal is for authorized Medicaid employees to receive the highest quality data for the Agency's initiatives and purposes in accordance to the Enterprise Data Governance Data Quality Framework.

a. Policy
   i. Medicaid management and employees must be able to rely on data for information and decision support to perform daily business operations and meet the objectives of the data strategy.
   ii. The DGO shall establish a Data Quality program to develop a governed approach for ensuring data is fit for use by Medicaid management and employees.
   iii. The activities of the DGO may support the development of high-quality data, and the Data Quality Program must support and sustain a governed data environment. Medicaid data must be:
      1. Valid
      2. Reliable
      3. Accurate
      4. Timely
   iv. The Data Quality program may require the definition of standards and specifications for data quality controls as part of the data lifecycle. Standards and specifications will align with business rules defined by the users of the data.
   v. The Data Quality program may define and implement processes to measure, monitor, and report data quality levels.
   vi. The principles guide of the Data Quality Program is in accordance to the DGO Operation Procedures

3. Data Access Policy

The objective of the Data Access policy is to facilitate and coordinate the sharing of data and information among its members, and continually enhance efficiency and consistency in collecting and exchanging data. Alabama Medicaid Agency at the enterprise level shall protect the privacy and confidentiality of individuals.

The Data Access policy ensures Medicaid employees and business associates have appropriate access to organizational data and information, as required by their job responsibilities. It focuses on improving processes for obtaining and managing access to data while adhering to the HIPAA principle of "minimum necessary." The goal is to maintain appropriate levels of security and access to protected information while minimizing the impact that data access can have on Medicaid operations. The policy applies to all Medicaid employees, Medicaid business associates and their employees, and all uses of Medicaid data, regardless of the programs or format in which the data

reside. The Data Access Policy incorporates the following strategies to achieve its objectives through the EDG Data Security Framework.

    a. Data Security
- i. Policy
  1. The DGO shall collaborate with the Information Security Office to establish security classifications for data elements within all Medicaid data assets.
     a. Security classifications shall describe the sensitivity of the data element and the likelihood as if pursued for malicious purposes.
     b. Classifications shall determine who can access the data.
     c. The highest security classification of any data element within a set of data shall determine the security classification for the entire set.
  2. The DGO may establish policies and practices for securing data that align with those implemented by the Medicaid Information Security Office.

    b. Data Sharing

The objective of the data sharing process shall be standardized, controlled, and monitored to ensure that the Alabama Medicaid shares the right data with the right people at the right time, without placing unnecessary or unauthorized risk on our recipients or the Agency.

- i. Policy
  1. DGO will serve as the focal point for guidance, direction and oversight of Alabama Medicaid data sharing initiatives.
  2. Data Sharing and Confidentiality Rules shall be set for the management of information sharing between Alabama Medicaid Agency and other agencies and organizations.

    c. Data Use
- i. Policy
  1. Personnel must access and use data only as required for the performance of their job functions, not for personal gain or other inappropriate purposes.
  2. The DGO shall collaborate with the Information Security Office to establish safeguards to protect the confidentiality, integrity and availability of individually identifiable and protected health information. The Information Security Office may periodically review user activity logs and documents to validate compliance with security regulations, policies, and standards.

     a. Access
        i. Authorized users shall have the goal to receive timely access to data and information systems.
        ii. Data use policies and practices shall align with the "minimum necessary" standard defined by HIPAA.
        iii. The goal is to apply the highest level of protection for Medicaid data assets in a manner that does not interfere with the efficient execution of Medicaid's business processes.

   b. Authorization
     i. Medicaid employees may obtain access only to specific views of data that are appropriate for their role within the organization.
     ii. Authorization for access to Medicaid data assets shall be in accordance with policies established by the Information Security Office.
   c. Authentication
     i. Whenever possible, authorized users shall obtain verification by the program that stores the data before gaining access to Medicaid data assets. Data stored in a flat-file or application that does not support separate authentication, the users shall authenticate by file permissions.
     ii. Authentication must occur each time the user accesses the data or information.
  3. This policy applies to all users of Medicaid data, regardless of the programs or format where the data reside.
  4. Anyone who is subject to this policy according to the Personnel Sanctions policies of the organization and fails to comply shall be in deem of violation and may be subject to disciplinary or legal action.

4. Analytic Prioritization Policy

  a. Policy
    i. The DGC may collaborate with the Commissioner, the CDO, Division Directors of Analytics and Informatics, and others as deemed appropriate to develop the strategic analytic plan for Medicaid.
    ii. The DGC, through the DGO and DGCM, shall implement the requirements of the strategic analytic plan.
    iii. To manage the demand for analytic services, the DGC may balance top-down priorities with bottom-up requests from business units by advocating resource allocation between centralized and decentralized analytic resources.

5. Data Content Policy

  a. Policy
    i. The DGC may review and approve the enterprise Data governance, data acquisition, and data management strategies.

6. Data Literacy Policy

  a. Policy
    i. The DGO may develop initiatives to increase data literacy among Medicaid employees.
    ii. The DGO shall implement training to:

1. Teach users how to distinguish good data from bad data in the context of their role within the organization. The goal is to increase the accuracy and efficiency of decision-making processes.
2. Promote the understanding and efficient use of data analysis tools.
3. Use Medicaid data to develop process improvement techniques
4. Implement statistical techniques to improve decision-making when data is incomplete or scarce.
5. Collect and disseminate metadata, especially that which is associated with the Enterprise Data Warehouse ("EDW").
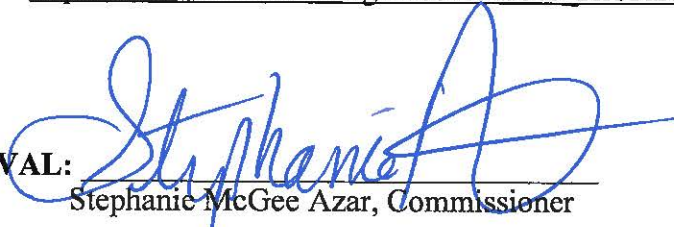
As Medicaid progresses in analytic maturity and data utilization, these policies shall likewise evolve to ensure its effectiveness and efficiency.

7. **Related AIMs, Data Governance Charter and Policies**
   The following AIMs and Medicaid policies relates to this AIM:
   - Data Governance Charter and Standard Operating Procedures
   - Alabama Medicaid Agency Internal Memorandum No. 201: Request for Information
   - Alabama Medicaid Internal Memorandum No. 206: Release of Confidential Information
   - Alabama Medicaid Internal Memorandum No. 216: Compliance with Federal and State Legislated Security and Privacy Requirements – risk-based approach
   - 45 C.F.R. Part 95 Subpart F - Automated Data Processing (ADP) Equipment & Services (available at https://www.ecfr.gov/cgi-bin/text-idx?SID=21403ec6a15b832070157eae96f6d7d1&mc=true&node=pt45.1.95&rgn=div5)
   - Alabama Medicaid Agency Administrative Code Rule 560 (available at https://medicaid.alabama.gov/content/9.0_Resources/9.2_Administrative_Code.aspx)

APPROVAL: _____
Stephanie McGee Azar, Commissioner

HISTORY: **May 1, 2020**

RESPONSIBLE UNIT: Data Governance Office