State of Tennessee

Division of TennCare

Data Policies and Standards

Version: 2.0
Submitted Date:
04/06/2022

Table of Contents

Table of Tables

1. Executive Summary

The Data Policies and Standards defined in this document are intended to provide direction for how TennCare's data assets should be managed and maintained to better meet data-related regulatory requirements and align with TennCare's vision, mission, and member service and health care delivery goals. The defined Policies and Standards are intended to be broad and provide references to more detailed standards and documents, as applicable.

This Data Policies and Standards document is comprised of ten sections that together dictate the detailed governing of TennCare's data related activities. The nine sections include:

- Introduction – This section provides the details behind the purpose of this document and the overall objectives for establishing these Policies and Standards, including the identified scope and constraints.
- Data Creation & Maintenance – This section describes how new data should be established and how existing data should be maintained to ensure it remains reliable for users.
- Master and Reference Data Management – This section describes how Master and Reference Data should be managed and maintained.
- Metadata Management – This section defines Metadata as it relates to TennCare and how the types of Metadata should be managed and maintained.
- Data Integration and Controls – This section encompasses the Policies and Standards as they relate to how data is transmitted and received by modules and repositories at TennCare.
- Data Quality – This section defines various data classifications and requirements and includes the Policies and Standards necessary to achieve the identified data requirements.
- Data History – This section contains the Policies and Standards as they relate to TennCare's data history requirements.
- Defining and Capturing Data Requirements – This section describes how data requirements should be captured during the overall development process.
- Test Data - This section specifies how test data will be managed for solution projects.
- Appendix – This section, which is comprised of three separate appendices, contains the Data Management Plan Outline, Referenced Documents, and Definitions and Acronyms.

2. Introduction

TennCare is the agency charged with the State of Tennessee's (the State) Medicaid program, CoverKids program, the Office of eHealth Initiatives and the Strategic Planning Initiative Group and is directed by the Department of Finance and Administration (F&A).

TennCare operations are a highly outsourced, multi-vendor ecosystem that manages multiple systems with large amounts of data. TennCare's data is subject to many requirements and standards from Federal and State agencies and regulations (e.g., Centers for Medicare and Medicaid Services [CMS], Internal Revenue Service [IRS], Social Security Administration, F&A, HIPAA/HITECH, Title 42 Part 2, T.C.A. 33-3-103) that, if violated, could result in lawsuits and penalties and that could severely affect TennCare operations.

2.1 Purpose

The purpose of this document is to define and describe TennCare's Data Policies and Standards that must be met in the conduct of data-related activities governed by TennCare. This document also:

- Provides guidance and direction on how data should be managed and maintained within the State.
- Provides data management guidance and direction for system implementers, integrators, and vendor partners.
- Provides a centralized location and reference for data management guidance and direction.

2.2 Objective

The objectives of establishing and adhering to data Policies and Standards are to:

- Support TennCare in conforming to federal and state regulations.
- Improve enterprise data quality.
- Protect data assets; prevent data loss.
- Improve data sharing and interoperability between TennCare applications and modules.
- Improve data sharing and interoperability between TennCare and other agencies, organizations, and partners.
- Improve efficiency and reduce costs of system/application development and maintenance.

2.3 Scope

2.3.1 In Scope

This section provides a description of what is in scope of the Data Policies and Standards.

2.3.1.1 These Policies and Standards apply to employees, agents, contractors (inclusive of subcontractors and pass-through), and consultants performing work within or on behalf of TennCare (Enterprise).

2.3.1.2 These Policies and Standards apply to all data management and data governance activities.

2.3.1.3 Unless otherwise noted these Policies and Standards apply to the scope of the changes including all data referenced within the scope of change that is input to, created by or persisted by information systems built for the Enterprise, whether by TennCare or by third parties, and any modifications the Enterprise may make to the purchased commercial off-the-shelf (COTS) systems. These Policies and Standards should also be used as evaluation/purchase criteria for COTS and exceptions for purchased COTS should be escalated through the TennCare Executive Data Governance Committee (TEDGC).

2.3.1.4 These Policies and Standards also apply to data within the scope of all system-to-system interfaces between systems, whether built internally, built externally, or purchased COTS systems.

2.3.1.5 In the event the scope of change for a project affects more than 50% of a given system, the TennCare Data Governance Organization (TDGO) may decide at its discretion to apply these Policies and Standards to the entire system.

2.3.1.6 These Policies and Standards apply to structured and unstructured data unless otherwise noted.

2.3.1.7 The Policies and Standards apply to all data irrespective of the hosting mechanism for the data – on premise, cloud, or vendor managed hosted services.

2.3.2 Out of Scope

This section provides a description of what is out of scope of the Data Policies and Standards:

2.3.2.1 These Policies and Standards do not apply to projects that have completed development as of the effective date of these Policies and Standards.

2.3.2.2 These Policies and Standards do not apply to production Information Technology (IT) systems implemented prior to the Policies and Standards approval, beyond the change activities referenced in this document.

2.3.2.3 Unless the data is comingled with other in scope data, these Policies and Standards do not apply to information collected, used, or generated for litigation and investigation purposes, or systems used by the legal department specifically for managing and processing information for litigation and investigation purposes;

or other information or systems that are protected by the attorney-client privilege, the work product doctrine, or other similar legal privileges or doctrines.

2.3.2.4 Supporting materials, such as principles, processes, procedures, templates, and other guidance documentation may be referenced and are maintained outside of these Policies and Standards.

2.4 Risks and Constraints

2.4.1 Risks

The following risks apply to the TennCare Data Policies and Standards:

2.4.1.1 The schedules of system implementers, integrators, and vendor partners may require realignment with respect to data related activities if their implementation plan differs from the State's requirements contained herein.

2.4.1.2 COTS products and Managed Services may limit the ability to meet the Policies and Standards as described in this document.

2.4.2 Constraints

The following constraints apply to the TennCare Data Policies and Standards:

2.4.2.1 Please refer to Out of Scope section

3. Data Creation & Maintenance

Data should be strictly controlled coming into the TennCare enterprise, and once it is in the Enterprise, a System of Record (SOR) should be identified for each data element. Changes to the data element should be made at the SOR and then communicated to data users. This section enables common definitions and rules for SOR so that data users can have known reliable sources of data. This section also provides a standard approach to create new data, make data changes, and to propagate and communicate data changes. This section applies to all types of data, including derived data, unless otherwise noted.

3.1 Standard Definitions and Guidelines for SOR

3.1.a Data should be assigned to one or more of the following categories as applicable:

- Master Data –data that is shared and required across business areas, processes, and systems and is a key dimension for aggregation in a data warehouse or analytical data store (see Master and Reference Data Management for more information and examples).
- Reference Data – data that is used to organize, categorize, or list permissible values of data. It usually consists of codes, abbreviations, and definitions and is constant, or seldom changed (see Master and Reference Data Management for more information and examples).
- Transaction Data – data that results from a business event, such as an encounter, claim, enrollment, or other business event.
- Derived Data – data that results from a transformation or aggregation of other data (ex. aggregative data from an analytical warehouse).
- Metadata – data that is about data. It's a structured description of data characteristics reflecting the meaning, content, structure, usage, and purpose of a data object (see Metadata Management for more information and examples).

3.1.b Data ownership and accountability should be assigned and executed per the TDGO charter.

3.1.c If current data should be corrected after set up, data should be corrected in the SOR and the system should enforce the business rules used at set up. This includes data validation rules such as edits, default values, and referential integrity rules. For data deemed to be critical to the Enterprise, an audit trail should be maintained for changes. For non-critical data, audit trails should be maintained based on system requirements.

3.1.d To facilitate the identification of changed records, the SOR should persist the following information for each record: the name of the User or the system who changed the data and the date and time when that change occurred. Changes include creating, updating, or deleting data.

3.1.e When a data value is corrected after set up, changes should be communicated and available to all end users.

3.1.f The SOR should be defined for each individual data element.

3.1.g The SOR should include functionality to correct data through a system interface, rather than through manual or scripted changes to the database that might bypass security and data validation rules enforced by the system.

3.1.h If derived data is required by a downstream system or user, the derived data elements should be persisted. The system that initially creates the derived data element should become the SOR for that data element and the users should reference that element from the SOR. Systems, other than the SOR, should not recreate intermediate results that were not persisted by the SOR.

3.1.i Business data that provides information in support of a business event or business decision should be persisted so that the Reference Data values effective at the point in time that the business event occurred can be retrieved later and associated with the event.

> For example, when a new diagnostic code is created, relevant data about the diagnosis also might need to be shared with downstream Information Systems and Users to process this event.

3.1.j Data parameters that impact the data values persisted by the SOR should be persisted such that the parameter values in effect at a point in time can be determined. The parameter data, for example, may include the dates specifying a period of time or the factors used to calculate projections.

3.1.k Additive data, data that is typically summed to create a total billing amount for each service, should be changed using a cancel and correct approach, where the previous amount is negated and the new amount is added.

3.1.l Information sourcing is the process of obtaining information from an authoritative source, defined as the SOR, or an approved alternative data source that the organization has defined to provide specific information to data users, whether downstream systems or individuals, as appropriate. Data should be created or modified within authoritative sources.

3.1.m Data sources should be monitored and reviewed annually by the Managing Data Stewards to maintain security, sensitivity, and access classification and report compliance.

3.1.n Data security and sensitivity classification of the data sources should be published and easily accessible by TennCare users.

3.1.o Data users and the business projects, systems, and processes should use business information only from approved authoritative source(s).

3.2 Data Corrections

3.2.a Systems should include the ability for data users to make changes to data in a controlled manner. Legacy systems do not always have this capability; however, it is still sometimes necessary to make deletions of business data in a production environment. These changes should follow a defined change management process and notification.

3.2.b A tracking tool should be used to log, track, and report requests, changes, and approvals of Data Corrections. See the Critical Data Elements Process for additional details on Data Corrections tracking.

3.2.c Data Corrections should be made at the SOR and propagated to all data users. Once corrected at the SOR, the downstream systems should reflect the correct data post-correction.

3.3 Data Purge, Archive, Retention

3.3.a Data retirement involves the disconnection of any interfaces or ongoing access to the designated data and the archival or purge of that data.

3.3.b A process for both archiving and purging data should be in place in accordance with all pertinent retention policies, standards, and guidelines, as well as regulatory and legal requirements and Non-Destruct Policy and retention policies issued by the State or Division of Health Department. These include but are not limited to:

3.3.c TennCare Records Retention Policy

3.3.d TennCare Records Disposition Authorization (RDA) List

3.3.e Data retirement, purge and archiving rules should be fully documented, traced, and logged with the TDGO. Locations of archives should be registered, dated, and maintained by the respective business units or records custodians.

3.3.f Retirement, purging and archival rules and significant changes should be reviewed and approved by the TDGO.

3.3.g Data archival should include enough context and metadata so that the data in the archive is usable if restored. Data archival should be based on a business unit of work and tied to a business event (e.g., a business unit of work might be defined as creation of coverage plans and a business event may be members enrolled within those plans.

3.3.h A data archive and the archive contents should be maintained in an archival catalog so that each archive can be located and identified as necessary.

3.3.i Records Management standards provide a legal framework for TennCare records retention. Additional guidance, templates, services, and training can be found at the Tennessee Records and Content Management. See also the Tennessee Records Retention policy.

3.3.i.1 All TennCare data governed by the TDGO should follow the aforementioned Records and Retention policies.

3.4 Data Conversion

3.4.a When converting data from existing solutions to updated or new solutions, the Data Conversion Standard shall be followed.

4. Master and Reference Data Management

Master Data is the data that is shared and required across business areas, processes, and systems and is a key dimension for aggregation in the data warehouse or analytic store.

Examples of Master Data include:

Provider: provider ID, name, address, type, specialty, location(s); and

Member: member ID, Name, correspondence address, billing address, phone number, etc.

Reference Data is used to organize, categorize, or list permissible values of data. It usually consists of codes, abbreviations, and definitions and is constant, or seldom changed. Examples include, State and Country Codes, Diagnostic Codes (ICD-9,10), CPT Codes, Member Status Codes (A-Active, I-Inactive), Member Relationship Codes (S-Self, DS-Dependent Spouse, DC-Dependent Child) and Currency (U.S. Dollar-USD, Australian Dollar-AUD, British Pound-GPB).

Master Data and Reference Data Management is managing the creation, modification, deletion, access, and usage of Master and Reference Data to:

- Meet the business needs of the enterprise
- Reduce duplication of data
- Act as trusted source of record for multiple consuming applications and data stores
- Maintain the quality of the data
- Govern the access to the data
- Reduce the cost of data integration
- Provide consistent aggregations, reporting, and analysis

4.1 Master Data and Reference Data Management Guidelines

4.1.a All data domains and data elements categorized as Master Data should comply with the following Policies and Standards to ensure the level of discipline and control required for Master and Reference Data:

4.1.a.1 All Master Data domains and elements should be required to have an assigned SOR as the Authoritative Source where the Master Data is created.

4.1.a.2 Data categorized as Master Data should be consistently defined throughout TennCare and any changes to definitions should be approved by the TDGO.

4.1.a.3 All downstream system consumers or data users should source and make use of Master Data from the SOR. (Note: the SOR may be an MDM data hub.)

4.1.a.4 All downstream business processes and data users should access the Master Data from the SOR to reduce duplication and ensure consistency.

4.1.a.5 Data categorized as Master Data should have specific access rights, data quality rules, and data quality thresholds documented, published, and maintained.

4.1.a.6 Data should be created, updated, purged, and maintained in the Master Data SOR.

4.1.a.7 To support controlled use of Master Data, Metadata should be supplied for each Master Data element as defined in as described in Metadata Management.

4.1.a.8 Master Data domains and/or data elements and associated Reference Data should be audited for data quality and TennCare Data Governance compliance on a quarterly basis. Exceptions found against the Master Data domains and/or data elements should have a remediation plan defined within five business days of the original audit exception findings.

4.1.a.9 Hierarchies should be standardized and the component information controlled and standardized. Some important characteristics of hierarchies should include the following:

4.1.a.9.1 Hierarchies should be consistently named and comply with existing standards.
4.1.a.9.2 Standard hierarchies should be used for regulatory reporting.
4.1.a.9.3 Hierarchies should have a consistent rollup structure. For example, the parent at any level should be at the same level for each named hierarchy. Similarly, children levels of parents should be at the same level for each named hierarchy.
4.1.a.9.4 All nodes of a hierarchy should be consistently named within that hierarchy.
4.1.a.9.5 To qualify as a hierarchy, the structure should have at least one parent and one child. Single nodes should not be used or classified as a hierarchy.
4.1.a.9.6 The use of alternate hierarchies require an exception from the master domain managing data steward and identification of the reporting purpose.

5. Metadata Management

Metadata is defined as data about data. It's a structured description of data characteristics reflecting the meaning, content, structure, usage, and purpose of a data object. There are different categories of Metadata including Business Metadata, Data Quality Metadata, Technical Metadata, Operational Metadata, and others as needed.

Metadata should be collected and standardized for all data domains and elements. As standardization across the TennCare ecosystem evolves, comparisons and trending Metadata will provide insight to the health and progress of the environment towards achieving TennCare's data governance and data quality objectives. The following Metadata should be defined and managed in a TennCare approved system or tool and reported and monitored by the TDGO.

5.1 Categories of Metadata

5.1.1 Business Metadata

The following Business Metadata should be defined, documented, monitored, and reported as appropriate:

- Business Name
- Business Definition
- Derivations and/or Calculations
- Authoritative Source(s)
- Data availability and refresh rates
- Data Ownership Roles, Owners, and Accountability
- Data Ownership Organization(s)
- Data Category (as described in Data Creation & Maintenance)
- Data Security Classification

5.1.2 Data Quality Metadata

The following Data Quality Metadata should be defined, documented, monitored, and reported as appropriate:

- Allowable values
- Data quality rules

- Data quality targets/objectives
- Data quality triggers
- Data quality scores

5.1.3 Technical Metadata

The following Technical Metadata should be captured, tracked, monitored, and reported as appropriate:

- Database (DB) Name and Internet Protocol/Uniform Resource Locator (IP/URL) or File name and path
- Schemas, Schema Description, Versions
- Tables, Table Description, Columns/Fields, Data Types, Index identification, Type of Key identification, Field Level Constraints, Field Description, Field Type – direct, derived
- Table/field relationships
- Data Transformation and Data Lineage from SOR to identified field
- Security at DB, Schema, Table and Column level
- DB or Table partitions and archiving settings
- Alias Information
- Volumetrics (table/database growth rates; current number of table rows; table usage characteristics; indexing structures)
- Aging/purge criteria

5.4.1 Operational Metadata

The following Operational Metadata should be captured, tracked, monitored, and reported as appropriate:

- Data generation and updating job schedule start date and time information
- Data generation and updating job expected completion date and time information
- List of jobs and job run sequences and dependencies
- Location of error logs

5.2 Data Models

Data models illustrate data concepts, entities, structures, and relationships at various abstractions and levels including conceptual, logical, and physical.

5.2.1 Conceptual Data Model

A conceptual data model is a summary-level model that describes the entire enterprise. The purpose is to organize, scope, and define business concepts, rules, and the relationships

between enterprise business areas. Although it may contain some attributes to provide context or clarification, the conceptual model doesn't provide complete details about the data elements involved.

5.2.2 Logical Data Model

A logical data model is a fully attributed model that describes data requirements from the business point of view and is technology neutral. The purpose is to develop a complete map of business rules and business concepts and provide a comprehensive description of the business. Logical sub-models may be organized around specific subject areas and integrated into an enterprise-level model.

5.2.3 Physical Data Model

A physical data model is a representation of a data design proposed or implemented in a specific database management system. Derived from the logical model, a physical model includes the definition of database management system-specific structures and implementation-specific attributes such as domain, length, constraints, and performance-oriented attributes such as storage location, indexes, and partitioning. It may also contain security and access control attributes. The physical model can also extend the logical model to include specialized data elements for system support and performance enhancements.

5.2.3.1 Data models should be created, updated, and maintained per the TennCare Enterprise Architecture Modeling Standard.

5.2.3.2 Data models should be managed and maintained per the TennCare Systems Implementation Lifecycle Process (SILC).

6. Data Integration and Controls

Data integration addresses how data is transmitted to and received by modules and repositories.

6.a Data interfaces and exchanges should be implemented using the data standards referenced above.

6.b The mapping and business rules for data movement between systems should be documented and published in a central and accessible Metadata repository.

6.c Data movement from one IT-supported data store to another is automated and verified for completeness and accuracy using automated controls that compares data in the source to data in the target.

6.d These controls should include, at a minimum, the detection, notification, and management of exceptions when moving information from source to target.

6.e PHI and PII data should be encrypted both at rest and while in motion from source to destination.

6.f Exceptions should be escalated to the TDGO base.

7. Data Quality

Data quality is a measure of data's satisfaction of its intended purpose and requirements. Data quality measures should have the following classifications and characteristics.

7.1 Data Quality Classifications

Table 1: Data Quality Classifications

Data Quality Classification	Data Quality Characteristic Description
Accuracy/Correctness	The degree of agreement between a data value (or set of values) and a source assumed to be correct. The source may be a reference set obtained by comparison to "real world" data, or by reference to a data set on another system or file that is deemed "correct".
Completeness	The degree that the full values are present in the attributes that require them, and the degree that the attributes cover the user data requirements.
Timeliness/Currency	Currency measures how up-to-date the data is, and whether the data required can be provided by the required time.
Consistency/Uniqueness (No Duplicates, Integrity)	Consistency is the extent that there is a single representation of data. Consistency also includes the extent that data is duplicated within a system, e.g., duplicate member names due to marriage, separation, and changes in household. The ability to establish the uniqueness of a data record (and data key values).
Validity	The data is stored in an acceptable format and is within a reasonable range of possible values.
Accessibility	Ability for users to extract the existing data they require. Users should not have different interpretations of the same data.

7.2 Data Quality Standards

7.2.a IT systems should load or update a data attribute only with data that conforms completely to the definition of that data attribute.

7.2.b Preventative and detective data quality controls should be implemented in systems based on business requirements. Preventative controls should prevent data with invalid values from being entered into an SOR. Detective controls should identify errors and enable data updates that address the errors.

7.2.c Data quality issues should be monitored, logged, and tracked through common, standard tools as defined by the TDGO. The TDGO should review these data quality issues regularly and escalate them as needed for resolution.

7.2.d Data quality metrics, standards, targets, and acceptable data quality thresholds to which enterprise data elements should conform should be defined. Data quality performance should be reported on at least a monthly basis. See the Critical Data Elements Process for additional reporting details.

7.2.e The Managing Data Stewards should request a review of the data quality checks with the Technical Data Stewards to ensure the integrity of the core data elements is maintained throughout the lineage of the data in the TennCare enterprise.

7.2.f Data quality rules should be collected, validated, reconciled, and maintained. These rules should be reviewed quarterly by the TDGO. See the Critical Data Elements Process for additional data quality rule process details.

8. Data History

The Policies and Standards in this section apply when requirements specify that data history is required.

8.a Data history should capture original values as well as changes.

8.b Data history should be insert only (cannot be updated or deleted). Any changes or corrections should create a new history record that is date-and-time stamped. If the history should record multiple changes that can occur within a day, each version should record the time the current values are persisted and the time that the values are replaced with new values in addition to the above dates. The latest update date and time stamp indicates the most current record. These time and date attributes enable values from a specific point in time to be retrieved. No destructive changes to the data are permitted, such as updating the business data in place.

8.c Versions in a data history should not be physically deleted when data is deleted in the SOR; instead the data in the data history should be logically deleted.

8.d "For example, when individual records are deleted from an SOR, a delete flag indicator can be set to designate that the record is logically deleted instead of physically deleting the record.

8.e Data history should be traceable to the SOR(s) regardless of the location of the SOR.

9. Defining and Capturing Data Requirements

Data requirements for new and modified business capabilities should be defined precisely enough to verify that systems, interfaces, and databases are designed and constructed in a way that includes and satisfies governance Policies and Standards. Business data requirements for new projects should adhere to the governance deliverables specified in the life-cycle applicable to the project (e.g., Waterfall, Agile, etc.) and include:

9.a Detailed data requirements that describe the information that the business needs (e.g., plan name, provider name, plan number, provider ID, member/client ID, MMIS ID etc.) with context necessary to understand what is being referenced (e.g., planning flag is an insufficient requirement but planning flag for an organizational change provides context needed for understanding).

9.a.1 "Information that the business needs" includes data acquired, consumed, produced, or published within a business "event"/activity.

9.b During the project requirements phase, Managing Data Stewards, Technical Data Stewards, data suppliers, and data consumers should be identified to assist in defining and reviewing data requirements for aster data, reference data, metadata, transaction data, and derived data.

9.c Process data requirements should describe how each process uses the information described in the project's detailed business data requirements, including the governance of information, how current the data needs to be, whether the process creates or updates data, and how long data should be retained to meet the needs of the business process, as well as regulatory and legal requirements. Business "events"/activities should include an owner and the producing and/or consuming events as well as the data associated with each event and the ownership.

9.d Business requirements that are traceable to physical implementation, including to every physical database and data feed created or used by a project, should be approved by the TEDGC.

9.e Data requirements should include Master and Reference Data, Metadata, and data quality requirements described in previous sections.

10. Test Data

Test Data information is to be updated based on the *TennCare Test Management Standard* document.

The finalized Solution Test Plan (section 6.2) shall specify how test data will be managed for its solution project. TennCare will assist the solution vendor in planning for and obtaining needed test data. TennCare Privacy and Security approval is required prior to sending any sensitive data or production data to a vendor. Table 3 lists the specifications required and additional considerations that provide guidance to solution vendors on TennCare's expectations for managing test data and the testing process:

Table 2: Test Data Specifications and Considerations

Test Data Specifications	Guidance about Test Data
Test data approval	TennCare approval of a solution vendor's Test Plan, addressing the data specifications listed below, is required prior to extracting any production data or sensitive data for testing.
Test data elements required	Names of the databases, tables, and fields to be extracted. Specify selection criteria and any referential integrity required between tables.
Test data extraction	The vendor shall work with TennCare or associated database administrators (DBAs) to extract, transform, and load data into the test environments as appropriate.
Test data transformation	Transforming test data (including cleansing and de-identifying it) may be the responsibility of the solution vendor, an IS Vendor or TennCare, depending on how data will be shared.
Test data cleansing	Consider whether the tests need cleansed data. Data with realistic quality issues may be needed to test how the solution handles errors and inconsistencies.
Test data de-identification	Only PROD and PREPROD environments can use real data without de-identification. De-identify PII, PHI, FTI, and other sensitive data where necessary Specify which fields need to be de-identified. Provide a detailed methodology and documentation of the rules for de-identifying in the Master or Solution Test Plan. Consider algorithms that keep the data realistic, to maximize how much testing can be done with de-identified data. Ensure that the de-identification method is suitable for integration testing across modules and vendors, where applicable.
Test data access	Designate which personnel will be authorized to see sensitive data when managing data, conducting tests, or viewing test results.

Test Data Specifications	Guidance about Test Data
Test data security	For tests that must be conducted with sensitive data, ensure full security compliance measures are applied to the test databases, environments, and personnel.
Test data loading	See the RACI chart for responsibilities for managing shared test environments, including loading test data to those environments.
Test dataset tracking	Use a tool to track the test datasets loaded to any environments. Track dataset versions, refreshes, updates, and test datasets created by other tests.
Test data identification in results	Test results shall track which test dataset version was used to run the test to help with defect management. Testing oversight may use this information to monitor and plan data "fixes" that enable a test to succeed.
Test data refreshes	Specify the frequency of refresh required for each test dataset. During the testing process, if testing data is modified with both successful and failed tests, the data gradually becomes less realistic. Periodically, the test data can be refreshed with a "gold copy" snapshot of production data (de-identified as appropriate). Data refreshes must be coordinated, scheduled, and communicated to all users of the test environment to avoid interrupting an in-flight test or yielding false test results. To support O&M testing and Decommissioning activities it is recommended to continue refreshing the test data after Go-Live.
Test data backups	Specify the frequency of backups required for each test dataset.
Test data retention and deletion	Specify whether, how and for how long each dataset will be retained, archived, or securely deleted. A dataset might be retained for use in a subsequent testing stage or for later testing of fixes and regression testing. A dataset might be archived, such as by removing it from a test environment but storing it for reference in interpreting test results. A dataset might be deleted at the end of a stage or after the solution project is completed.

10.a The review and approval of each test dataset shall be tracked by TennCare, using the following data elements:

- 10.a.1 Test data unique identifier
- 10.a.2 Test data version (and description if appropriate)
- 10.a.3 Status, with values to include In review, In revision, Approved
- 10.a.4 Revisions required (description)
- 10.a.5 Date dataset and uses approved
- 10.a.6 Approver information (Person name and Organization role)

10.b The approved version of the test dataset shall be captured and linked to the approval record.

11. Appendix A: Data Management Plan Outline

11.A.1 The following outline is a guide for the structure of the Data Management Plan that must be delivered during the Design phase of a TennCare project. This document describes how all the data within the scope of the project will be managed throughout its lifecycle, including data requirements. The document must describe how data and data requirements will be planned, executed, monitored, and controlled within a project.

11.A.2 The Data Management Plan may point to other documents where data management components are being described in further detail, such as the Test Plan or the Technical Design Document. The table within the outline below maps which components of data management must be addressed and where they can be described. The Data Management Plan consolidates a complete map of data needs across the entire project scope.

11.A.3 This plan will also either contain or will point to the document(s) where data requirements are described and how they will be managed across their lifecycle. Data requirements can be described through requirements statements or conceptual and logical data models. Data requirements must be managed like business or system requirements and must be planned, executed, monitored, and controlled.

11.A.4 Data Management Plan Outline:

11.A.4.1 Document Purpose

11.A.4.2 Data Requirements

- Definition
- Lifecycle (states) of the data requirements
- How data requirements will be represented in the project (e.g., through a Requirements Traceability Matrix, Conceptual, Logical and Physical Data Model, etc.)
- Traceability of data requirements to Contract Requirements

11.A.4.3 Data Management Deliverables Aligned to the Solution Implementation Life Cycle, Data Policies and Standards, and the Test Management Standards

Table 2: Data Management Deliverables Aligned to the Solution Implementation Life Cycle (SILC)

Standard	Section	SILC Phase	Relevant Deliverable
Data Policies and Standards	External Policies and Standards	Requirements Review	Requirements Traceability Matrix
		Design	Technical Design Document

Standard	Section	SILC Phase	Relevant Deliverable
Data Policies and Standards	Data Creation & Maintenance	Design	Systems Security Plan Technical Design Document
		Development	Operations Run Book
Data Policies and Standards	Master & Reference Data Management	Requirements Review	Conceptual Data Model
		Design	Technical Design Document Data Conversion Management Plan Logical Data Model Physical Data Base Design
		Development	Physical Data Model and Dictionary Operations Run Book
Data Policies and Standards	Metadata Management	Design	Systems Security Plan Technical Design Document
		Development	Operations Run Book
Data Policies and Standards	Data Integration & Controls	Design	Interface Control Design Document Integration Plan Technical Design Document
Data Policies and Standards	Data Quality	Design	Technical Design Document Data Conversion Management Plan
		Development	Operations Run Book
Data Policies and Standards	Data History	Design	Technical Design Document
		Development	Operations Run Book
Data Policies and Standards	Defining & Capturing Data Requirements	Requirements Review	Requirements Traceability Matrix
		Design	Data Conversion Management Plan
Test Management Standards	Test Data	Design	Test Management Plan

11.A.4.4 Tools and Repository (how will data related artifacts and deliverables be managed in the different tool sets)

11.A.4.5 Data Management Roles and Responsibilities (RACI)

11.A.4.6 Data Management Reporting (reporting on the state of data requirements and data management in the project, independent of deliverables)

11. Appendix B: Referenced Documents

These documents and other sources of information are referenced throughout this policies and standards document and include federal, state and TennCare sources potentially applicable to agency data practices.

Table 3: External Referenced Documents

#	Document Name and Link	Description
1	Center of Medicare and Medicaid Services – Medicaid Information Technology Architecture (MITA) Information Architecture	Contains the details and framework of the MITA information architecture
2	Center of Medicare and Medicaid Services – Behavioral Health MITA	Introduces the Behavioral Health MITA Business Process/Data Model
3	Medicaid IT Architecture's (MITA) Information Architecture (IA) Part II Chapter 5 Data Standards 3.0	Collection of MITA documents that outline the MITA information architecture, data management strategy, conceptual data model, logical data model, data standards, and information capability matrix
4	Minimum Acceptable Risk Standards for Exchanges (MARS-E) v2.0	Presents the security and privacy controls necessary and effective for managing ACA systems, data, and privacy in today's threat environment
5	IRS Publication 1075	Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of federal tax information
6	Health Information Technology for Economic and Clinical Health (HITECH) Act	The provisions concerning the privacy and security associated with the electronic transmission of health information
7	Children's Health Insurance Program Reauthorization Act (CHIPRA)	Outlines the legislative requirements of CHIPRA

8	Affordable Care Act (ACA)	Outlines the legislative requirements of the ACA
9	International Classification of Diseases, 10th revision (ICD-10)	Describes how ICD-10 codes and classifies mortality data from death certificates
10	Accredited Standards Committee X12N	Describes the standards-developing organization
11	Health Level 7 (HL7)	Describes the standards-developing organization
12	Current Procedural Terminology, 4th edition (CPT-4)	Details regarding the uniform coding system used to identify medical services and procedures furnished by physicians and other healthcare professionals
13	Diagnosis Related Group (DRG)	Describes the patient classification scheme
14	Healthcare Common Procedure Coding System (HCPCS)	Information related to the HCPCS, including coding processes and publications
15	Logical Observation Identifiers Names and Codes (LOINC)	Information on the common language (a set of identifiers, names, and codes) for identifying health measurements, observations, and documents
16	National Drug Code (NDC)	The history and directory for the NDC
17	Systematized Nomenclature of Medicine (SNOMED)	Information on the common global language for health terms

18	Americans with Disabilities Act (ADA) Section 508	Information on requirements outlined in Section 508 of the ADA
19	Web Content Accessibility Guidelines (WCAG) 2.0	Documentation on how make web content more accessible to people with disabilities
20	Electronic Health Records (EHR)	Information on what is captured in EHRs
21	Health Insurance Portability and Accountability Act (HIPAA) 5010 forma and security rule	Outlines the regulations introduced to the medical industry from HIPAA 5010
22	National Information Exchange Model (NIEM)	Describes the NIEM model of agreed-upon terms, definitions, relationships, and formats - independent of how information is stored in individual systems - for data being exchanged
23	National Council for Prescription Drug Programs (NCPDP) Standards	Information on the NCPDP standards
24	National Committee on Vital and Health Statistics (NCVHS) Standards	Information on the NCVHS standards
25	National Institute of Standards and Technology (NIST) Standards	Information on the NIST standards

26	National Uniform Billing Committee (NUBC) Standards	Information on the NUBC standards
27	National Uniform Claim Committee (NUCC) Standards	Information on the NUCC standards
28	American Dental Association (ADA) Standards	Information on the ADA standards
29	Dental Content Committee of the ADA (DCC) Standards	Information on the DCC standards
30	Council for Affordable Quality Healthcare – Committee on Operating Rules for Information Exchange (CAQH- CORE)	Information on the CAQH-CORE standards
31	Fast Healthcare Interoperability Resources (FHIR)	Information on the FHIR standards
32	Federated Health Information Model (FHIM)	Model used to describe a vast amount of federal health-related information

Table 4: TennCare Referenced Documents

#	Document Name	Description
1	TennCare Systems Implementation Lifecycle (SILC) Process	Defines the lifecycle process for solutions being developed for TennCare projects
2	TennCare Enterprise Architecture Modeling Standard	Defines the TennCare enterprise architecture and the methodology used to manage the development of enterprise architecture artifacts
3	TennCare Data Governance Charter	Serves to ensure a common understanding of the TDGO
4	Information Security Policies	Contains the Tennessee IT data security policies
5	TennCare Records Retention Policy	The TennCare Records Retention Standards
6	Privacy and Compliance	Contains the Tennessee IT data security Policies and Standards to protect personal information and confidential organization information
7	Information Security Policies	TennCare information security policies
8	Privacy and Compliance	TennCare privacy and compliance policies
9	TennCare Data Naming Standard	Provide guidance on naming of data elements used by TennCare
10	TennCare Data Conversion Standard	Guides TennCare Vendor Partners and delegated project teams in the conversion of data from existing solutions to updated or new solutions
11	TennCare Data and Information Systems Classification Policy	Establishes the framework to be used by TennCare for assigning classification designations to data and information systems.
12	TennCare Records De-identification Policy	Addresses the processes through which “TennCare” will remove from agency records personally identifiable information (PII) or protected health information (PHI) as required by The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and or other relevant statutes.

13	TennCare Records Disposition Authorization List	Information on TennCare Records Disposition Authorization

11.B.1 These Policies and Standards are intended to work in concert with other State data, records management, and IT policies, and with federal CMS Policies and Standards. They do not supersede or replace any policy, regulation, law, or other mandate with which the organization should comply.

11.B.2 These Policies and Standards are intended to work in connection with MITA data standards (referenced in CMS MITA Framework 3.0, Part II Chapter 5 – "Data Standards") and guidelines provided by the CMS for the Medicaid program. The MITA framework is based on legislative requirements outlined in the HITECH Act, the CHIPRA, and the ACA.

11.B.2.1 The purpose of MITA data standards is to

- Enable data sharing and interoperability of Medicaid enterprise information.
- Support both a syntactic and semantic understanding of this information.
- Adopt healthcare industry standards governed by Designated Standards Maintenance Organizations (DSMOs).

11.B.2.2 MITA data standards identify the key components to be covered which include data element names, definitions, data types, and formatting rules. Data element names should describe objects, features, or data that are collected, automated, or modified by the business processes of a state agency's enterprise.

11.B.2.3 MITA data standards fall into two major categories: Structural data standards (Technical) and Vocabulary data standards (Business or Semantic).

11.B.2.4 MITA data standards include standards and data formats recommended by DSMOs for storage, transmission, and information interoperability.

11.B.2.5 International Standards include:

- ICD-10 data format
- Accredited Standards Committee (ASC) X12N with transactions like 270, 271, 275, 276, 277, 820, 834, 835, and 837 – Insurance data format
- HL7, FHIR, and Cross-Enterprise Document Sharing (XDS) data format for health information
- Vocabulary domains and code sets (for example, Current Procedural Terminology, 4th edition [CPT-4], Diagnosis Related Group [DRG], Healthcare Common Procedure Coding System [HCPCS], Logical Observation Identifiers Names and Codes [LOINC], National Drug Code [NDC], and Systematized Nomenclature of Medicine [SNOMED]), and Americans with Disabilities Act (ADA) Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0.
- Electronic Health Records (EHR) data format, if captured

11.B.2.6 National Standards prescribe capturing certain specific eligibility, enrollment, member, plan, benefits, provider, payer, third party, diagnosis, health, drug, claim, and billing information. This includes:

- Health Insurance Portability and Accountability Act (HIPAA) 5010 forma and security rule
- National Information Exchange Model (NIEM) standards for data exchange based on Extensible Markup Language (XML)
- HITECH Act protected health information (PHI) data usage

- CAQH-CORE national operating rules within the healthcare industry

11.B.2.7 Other DSMOs include:

- National Council for Prescription Drug Programs (NCPDP)
- National Committee on Vital and Health Statistics (NCVHS)
- National Institute of Standards and Technology (NIST)
- National Uniform Billing Committee (NUBC)
- National Uniform Claim Committee (NUCC)
- American Dental Association (ADA)
- Dental Content Committee of the ADA (DCC)

Interoperability standards apply to all MITA Information Architecture components that align to multiple data domains, including eligibility, enrollment, member/recipient, plan, program, benefits, provider, payer, third party liability, care and case management, contracts, rates, budget, claims/encounters, diagnosis, drug, billing, and utilization information.

A more comprehensive list of DSMOs and standards recommended by MITA is included in reference #3: Part II Chapter 5 Data Standards 3.0.PDF.

11.B.3 These Policies and Standards are intended to work in connection with existing State IT data security policies and TennCare data security Policies and Standards to protect personally identifiable information (PII), confidential organization information and control access to data for required and authorized roles. TennCare policies include:

11.B.3.1 Information Security Policies
11.B.3.2 Privacy and Compliance

11.B.4 Relevant federal security policies include:

11.B.4.1 MARS-E v2.0 - Minimum Acceptable Risk Standards for Exchanges IRS PUB 1075 (September 2016) – Tax Information Security Guideline11.

11. Appendix C: Definitions and Acronyms

Table 5: Definitions

Term	Definition
Accessibility	Data quality classification; ability for users to extract existing data they require
Accuracy/Correctness	Data quality classification; the degree of agreement between a data value (or set of values) and a source assumed to be correct
Additive Data	Data that is typically summed to create a total billing amount for each service
Alternate Hierarchies	A variation of a standardized hierarchy created for a different perspective
Cancel and Correct Approach	Method for changing additive data
Completeness	Data quality classification; the degree that the full values are present in the attributes that require them, and the degree that the attributes cover the user data requirements
Consistency/Uniqueness	Data quality classification; the extent that there is a single representation of data. Includes the extent that data is duplicated within a system.
Data Parameters	Factors and conditions that are used to form a particular population of data
Data Quality Manager	Monitors and improves data quality of critical data elements and guides the organizations units and data consumers/producers with regard to data quality activities
Data User	Downstream systems or individuals who utilize the data from the SOR
Derived Data	The result of a computational step applied to reference of event data. Derived data is the result of either relating two or more elements of a single transaction (such as an aggregation), or of relating one or more elements of a transaction to an external algorithm or rule.
Managing Data Steward	Accountable to operational team and end users to consider their input in defining minimum data quality requirements, and are accountable for implementing and administering those requirements as appropriate, including the administration of business rules and integrity conditions needed when data is created at the point of origination
Master Data	The information required to create and maintain an enterprise wide SOR for core business entities in to capture business transactions and measure results for these entities

Term	Definition
Metadata	Data about data. It's a structured description of data characteristics reflecting the meaning, content, structure, usage, and purpose of a data object.
Reference Data	Static, consistent, with a uniform set of identifiers and extended attributes that describe the core entities of the enterprise and are used across multiple business processes
Structured Data	Data that is structured, formatted and organized, which makes the data more easily searchable
System of Record (SOR)	System name of the authoritative source for a particular data element in a system containing multiple sources of the same element. To ensure data integrity, a single SOR should always exist for each data domain and data element.
Technical Data Steward	Ensures that data governance controls are implemented and monitored and works with the Managing Data Steward to maintain the required data quality
Timeliness/Currency	Data quality classification; the degree how up-to-date the data is, and whether the data required can be provided by the required time
Transaction Data	An event involving the exchange (or modification) of products, money and/or data. The transaction has meaning to the business.
Unstructured Data	Data that is unstructured and not organized in a pre-defined way, which makes the data more difficult to search
Validity	Data quality classification; the extent the data is stored in an acceptable format, and is within a reasonable range of possible values

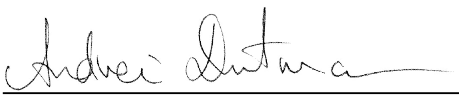
Table 6: Acronyms

Acronym	Definition
ACA	Affordable Care Act
ADA	Americans with Disabilities Act
ADA	American Dental Association
ASC	Accredited Standards Committee
CAQH-CORE	Council for Affordable Quality Healthcare – Committee on Operating Rules for Information Exchange
CHIPRA	Children's Health Insurance Program Reauthorization Act
CPT-4	Current Procedural Terminology, 4th edition
DB	Database
DCC	Dental Content Committee of the ADA
DRG	Diagnosis Related Group
DSMO	Designated Standards Maintenance Organization
EHR	Electronic Health Records
F&A	Department of Finance and Administration
FHIR	Fast Healthcare Interoperability Resources
HCPCS	Healthcare Common Procedure Coding System
HIPAA	Health Insurance Portability and Accountability Act
HITECH Act	Health Information Technology for Economic and Clinical Health Act
HL7	Health Level 7
IT	Information Technology
ICD	International Classification of Diseases
IP	Internet Protocol
IRS	Internal Revenue Service
LONIC	Logical Observation Identifiers Names and Codes
MARS-E	Minimum Acceptable Risk Standards for Exchanges

MCO	Managed Care Organization
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
NCPDP	National Council for Prescription Drug Programs
NCVHS	National Committee on Vital and Health Statistics
NIST	National Institute of Standards and Technology
NUBC	National Uniform Billing Committee
NUCC	National Uniform Claim Committee
PHI	Protected Health Information
PII	Personally Identifiable Information
RDA	Records Disposition Authorization
SILC	Systems Implementation Lifecycle
SNOMED	Systematized Nomenclature of Medicine
SOR	System of Record
TDGO	TennCare Data Governance Organization
TEDGC	TennCare Executive Data Governance Committee
URL	Uniform Resource Location
WCAG	Web Content Accessibility Guidelines
XDS	Cross-Enterprise Document Sharing
XML	Extensible Markup Language

12. Sponsor Acceptance

Approved by the Data Governance Program Sponsor and a majority of Council voting members:



Date: 4/6/2022

Andrei Dumitrescu
Chief Data Officer

13. Revision History

Table 7: Revision History

Revision	Description of Change	Author	Date
1.0	Initial version of document	DG Team	3/24/2020
1.1	Updated document references	DG Team	4/2/2020
1.2	Updated document to add further detail around data retirement	DG Team	11/04/2020
2.0	Updated document to add further detail around Test Data, as well as to include the Data Management Plan Outline, and to update document location links	DG Team	4/6/2022

NDP066529-1A