CONTRACT
(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date	End Date	Agency Tracking #	Edison Record ID
September 1, 2022	August 31, 2029	31865-00852	75191

Contractor Legal Entity Name	Edison Vendor ID
International Business Machines Corporation (IBM)	0000000267

Goods or Services Caption (one line only)

Cloud-Based Data Ecosystem Data Quality (DQ)/Extract-Transform-Load (ETL) Pipeline

Contractor	CFDA #
☒ Contractor	93.778

Funding —

FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2023	$530,437.18	$4,773,934.59			$5,304,371.77
2024	$628,719.26	$5,658,473.36			$6,287,192.63
2025	$1,791,996.30	$14,194,579.97			$15,986,576.26
2026	$1,065,862.53	$7,014,913.87			$8,080,776.41
2027	$745,187.53	$4,128,838.87			$4,874,026.41
2028	$638,295.87	$3,166,813.87			$3,805,109.74
2029	$638,295.87	$3,166,813.87			$3,805,109.74
2030 (Option Year 1)	$481,805.08	$1,758,396.82			$2,240,201.91
2031(Option Year 1-2)	$429,641.49	$1,288,924.47			$1,718,565.96
2032(Option Year 2-3)	$429,641.49	$1,288,924.47			$1,718,565.96
2033(Option Year 3)	$107,410.38	$322,231.12			$429,641.50
TOTAL:	$7,487,292.98	$46,762,845.28			**$54,250,138.27**

Contractor Ownership Characteristics:

☐ Minority Business Enterprise (MBE):
☐ African American ☐ Asian American ☐ Hispanic American ☐ Native American

☐ Woman Business Enterprise (WBE)

☐ Tennessee Service Disabled Veteran Enterprise (SDVBE)

☐ Disabled Owned Business (DSBE)

☐ Tennessee Small Business Enterprise (SBE): $10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.

☐ Government ☐ Non-Minority/Disadvantaged ☒ Other: Corporation

Selection Method & Process Summary (mark the correct response to confirm the associated summary)

☒ Competitive Selection	RFP 31865-00619 was competitively bid.
☐ Other	Describe the selection process used and submit a Special Contract Request

Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.

Crystal Allen

Speed Chart (optional)	Account Code (optional)

CONTRACT

BETWEEN THE STATE OF TENNESSEE,

DEPARTMENT OF FINANCE AND ADMINISTRATION,

DIVISION OF TENNCARE

AND

INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM)

This Contract, by and between the State of Tennessee, Department of Finance and Administration, Division of TennCare ("State" or "TennCare") and International Business Machines Corporation (IBM) ("Contractor" or "DQ/ETL Contractor"), is for the provision of a cloud-based DE Component for the Data Ecosystem Solution, as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is A FOR-PROFIT CORPORATION

Contractor Edison Registration ID # 0000000267
Contractor Place of Incorporation or Organization: New York

A. SCOPE

A.1. The Contractor shall provide all goods or services and Deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.

A.2. Definitions. For the purposes of this Contract, definitions and abbreviations shall be as set forth in Attachment A, Definitions and Abbreviations.

A.3. The Contractor shall provide TennCare with a cloud-based Data Quality (DQ)/Extract-Transform-Load (ETL) Pipeline (DQ/ETL or DE Component) as part of TennCare's Medicaid Modernization Program (MMP)'s Data Ecosystem Solution (DE Solution). The DE Solution shall be comprised of four (4) Data Ecosystem Components (DE Components): Enterprise Data Warehouse (EDW), Data Quality (DQ)/Extract-Transform-Load (ETL) Pipeline, Master Data Management (MDM), and Decision Support System (DSS). The DE Component Contractor is responsible for providing and operating, as outlined in this Contract, the specified DE Component which shall incorporate current industry-standard tools and technology, shall be flexible to accommodate current trends, technological advances, industry-leading capabilities, and regulatory requirements, and shall be hosted in commercial public cloud infrastructure.

A.4. The words "Service" and "Services" as used in this Contract shall be as defined in Attachment A, Definitions and Abbreviations. References to specific Services, as opposed to all Services required under this Contract, may be inferred in each instance from the context of the Contract provisions.

A.4.1. The descriptions of Contractor Deliverables in this Contract do not include every possible duty, task, or intermediate deliverable necessary to achieve success on this Contract. The Contractor shall receive written approval by TennCare for Deliverables requiring TennCare approval to be effective. The Contractor shall be responsible for clarifying in writing any lack of detail it perceives in a specific area of work-or for a specific Deliverable-where it would appear to otherwise relieve the Contractor of a duty to conform with TennCare standards. This includes all intermediate steps, Deliverables or Processes reasonably necessary to achieve the desired outcome described in each Section of the Contract.

A.4.2. The Contractor shall work in conjunction with TennCare, Integration Services Contractor (IS Contractor), and Medicaid Modernization Program Vendors and Partners (MMPVP), and other DE Component(s) Contractor(s), if any, as necessary or at the request of TennCare, to coordinate and complete required activities and Deliverables. The Contractor shall coordinate with TennCare and MMPVP, and other DE Component Contractor(s), if any, to complete onboard services specific to

the Contractor's DE Component for Medicaid Management Information System (MMIS) Modules or systems provided by MMPVP through all phases of the Contract.

A.4.3. If applicable, TennCare shall designate the Enterprise Data Warehouse (EDW) Contractor to provide coordination for all four (4) DE Components and the DE Solution to include serving as an escalation point between the DE Component Contractor(s) and the orchestration and consolidation of required activities and Deliverables among the DE Components. If applicable, the individual DE Component Contractor(s) shall work in conjunction with the EDW Contractor, as necessary or at the request of TennCare, to coordinate, prioritize, and complete all requirements described in Section A.3 through A.5 and A.7 through A.13. Unless this Contract includes Scope of Services for the EDW, the EDW Contractor shall not be responsible for the services, Deliverables, materials, Special Project Change Orders, Special Project Enhancements, and any other work required to be performed by Contractor pursuant to this Contract.

A.4.4. Nothing in this Contract shall be deemed to be a delegation to the Contractor of the State's non-delegable duties under the TennCare program administered by the single state agency, as designated by the State and CMS, pursuant to Title XIX of the Social Security Act (42 U.S.C § 1396 et seq.), Section 1115 research and demonstration waiver granted to the State and any successor programs, or the Federal Children's Health Insurance Program (CHIP), known in Tennessee as "CoverKids," administered by the State pursuant to Title XXI of the Social Security Act.

A.5. Phased Implementation and Operation

A.5.1. Design, Development, and Implementation (DDI): The Contractor shall design, develop, and implement the DE Component and integrate into the comprehensive DE Solution that provides Enterprise-Wide data management, storage, and analytics for all Modules in the MMP. The implemented DE Component shall:

A.5.1.1. Meet the service and delivery timelines for DE Component DDI and DE Module Implementation DDI as specified in Contractor's project schedule. Any variances from these timelines, for any reason and whether approved by TennCare or not, will not result in additional cost(s) to TennCare.

A.5.1.2. Meet all Functional Requirements described in Sections A.6.

A.5.1.3. Meet all Non-functional Requirements described in Sections A.7 through A.13. DE Component DDI includes the integration of all Data Sources identified as described in Section A.6.3.1.2.

A.5.1.4. Comply with all applicable Service Level Agreements (SLAs) defined in Attachment B – Service Level Agreements and Liquidated Damages for DQ/ETL.

A.5.1.5. Be certified by Centers for Medicare and Medicaid Services (CMS), as required to receive Federal matching funds under 42 C.F.R 433 and 45 C.F.R 95. See SLAs in Attachment B – Service Level Agreements and Liquidated Damages for DQ/ETL, for Liquidated Damages associated with delays in, or failure to obtain, CMS Certification.

A.5.1.6. The Contractor shall be responsible for all data exchanges between agreed upon environments throughout DDI at no additional cost to TennCare.

A.5.1.6.1. The Contractor shall design components for data exchanges to be cost effective so that TennCare shall not incur any additional cost related to data portability expenses in a multi-cloud environment.

A.5.2. Operations and Maintenance (O&M) Phase

A.5.2.1. At the conclusion of DE Module Implementation DDI, the Contractor shall operate the DE Component as required by the O&M Phase, defined in Sections A.11.5.

A.5.2.2. The Contractor shall operate a Module Support Team for the DE Component as required by Section A.11.10.2.

A.5.2.3. The Contractor shall be responsible for all data exchanges between agreed upon environments throughout the O&M Phase at no additional cost to TennCare.

A.5.2.3.1. The Contractor shall design components for data exchanges to be cost-effective so that TennCare shall not incur any additional cost related to data portability expenses in a multi-cloud environment.

A.6. Data Quality (DQ)/Extract-Transform-Load (ETL) Pipeline The DQ/ETL Pipeline Contractor shall provide and operate a cloud-based DQ/ETL Pipeline that meets all requirements in this Section A.6.

A.6.1. Data Reconciliation Requirements

A.6.1.1.1. The DQ/ETL Pipeline shall have the ability to report on Data Reconciliation, identifying and alerting users of updates, possible data conflicts, and determine that the data pulled is complete and not duplicated.

A.6.1.1.2. The DQ/ETL Pipeline Contractor shall identify relevant critical data elements and develop automated reconciliation mechanisms for each Data Source in the Application and Interface Integration Inventory located in Attachment C, Procurement Library, in consultation with TennCare.

A.6.1.1.3. The DQ/ETL Pipeline Contractor shall implement tools to identify and investigate any data exchange discrepancies and work with the Source System for resolution prior to performing ETL processes.

A.6.2. Data Quality

A.6.2.1.1. The DQ/ETL Pipeline shall provide capabilities to support automated data profiling activities.

A.6.2.1.2. The DQ/ETL Pipeline shall provide reports for data profiling metrics including, but not limited to, completeness, consistency, conformity, integrity, duplication, accuracy, and list of values in intuitive reports, charts, and graphs.

A.6.2.1.3. The DQ/ETL Pipeline Contractor shall provide an ETL management tool that supports Data Quality management functionality with both automated and user-defined quality control capabilities.

A.6.2.1.4. The DQ/ETL Pipeline Contractor shall implement and enforce data management policies as described within the TennCare Data Policies and Standards for all enterprise Data Quality and governance processes, provide automated and manual Data Quality monitoring and improvement practices and procedures in collaboration with TennCare.

A.6.2.1.5. The DQ/ETL Pipeline shall have the capability to allow for reuse of the Data Quality rules through Application Programming Interface (API)-based integration with other applications in the TennCare Enterprise.

A.6.2.1.6. The DQ/ETL Pipeline shall perform Data Quality monitoring based on rules defined by TennCare and provide exception reports to any data determined to be out of compliance, as defined by the Data Quality rules following TennCare Data Policies and Standards guidelines.

A.6.2.1.7. The DQ/ETL Pipeline shall have the capability to validate data per the Data Quality dimensions found in the TennCare Data Policies and Standards.

A.6.2.1.8. The DQ/ETL Pipeline shall have automated quality checks and controls to regularly identify inconsistent, incorrect, and redundant values and shall report the identified data in the form of reports or alerts.

A.6.2.1.9. The DQ/ETL Pipeline shall have capabilities for creating, managing, and deploying Data Quality rules.

A.6.2.1.10. The DQ/ETL Pipeline Contractor shall resolve bad or otherwise corrupt data caused by the DQ/ETL Pipeline process in accordance to the Data Quality review process timelines, defined in the SLAs in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL. In addition, the DQ/ETL Pipeline Contractor shall coordinate and resolve with the Data Source provider and TennCare to address any bad or corrupt data generated by a Data Source as agreed upon during system design.

A.6.2.1.11. The DQ/ETL Pipeline shall be able to validate and troubleshoot in case of flaws or errors in the data through business rules and logic.

A.6.2.1.12. The DQ/ETL Pipeline shall include error and exception handling Processes that shall identify, filter and isolate the errant data.

A.6.2.1.13. The DQ/ETL Pipeline shall perform data cleansing and allow modification of data values, as per TennCare approved Data Quality rules to meet domain restrictions, integrity constraints or other Data Quality needs.

A.6.2.1.14. The DQ/ETL Pipeline shall have the capability to implement CMS-defined Tier 1, 2, and 3 top priority related Data Quality edits to proactively replicate T-MSIS abstracts applying Data Quality rule/validation rules based on CMS and TennCare guidance.

A.6.2.1.15. The DQ/ETL Pipeline shall have the capability to implement Data Quality rules/validation rules to allow for successful T-MSIS extracts.

A.6.2.1.16. The DQ/ETL Pipeline Contractor shall meet the established benchmark metrics, which can be used to measure DQ/ETL Pipeline performance set forth by TennCare on a monthly basis. The benchmark performance metrics will be mutually upon, in writing, by the DQ/ETL Pipeline Contractor and TennCare during the design phase and be part of the technical design document.

A.6.3. Data Integration

A.6.3.1.1. The DQ/ETL Pipeline shall have the following capabilities:

A.6.3.1.1.1. Connectivity, extraction, transformation and loading activities from various data structures (e.g. 3NF, dimensional, NoSQL);

A.6.3.1.1.2. Supports multiple formats of source data (e.g. flat files,.csv files, JSON, XML,); and

A.6.3.1.1.3. Collect data in the predefined file formats (e.g. fixed length file) from the Data Sources defined in the Data Ecosystem Application and Interface Integration Inventory.

A.6.3.1.2. The DQ/ETL Pipeline shall have the ability to integrate with multiple systems through the Integration Service Layer (ISL) – Enterprise Service Bus (ESB), including, but not limited to, Source Systems, external data file provider (such as Medicaid Managed Care contractors or State and Federal agencies), and downstream applications (such as the DSS).

A.6.3.1.3. The DQ/ETL Pipeline Contractor shall consult with TennCare and obtain approval to define the criteria/business rules required to create and manage data extracts.

A.6.3.1.4. The DQ/ETL Pipeline shall provide the capability to implement business rules defined by TennCare through reusable ETL transformation objects.

A.6.3.1.5. The DQ/ETL Pipeline shall provide both packaged and extensible rules for handling both syntax (formatting) and semantic (values) transformation of data to ensure conformance with business rules.

A.6.3.1.6. The DQ/ETL Pipeline shall be capable of receiving Data Sets from multiple identified TennCare Source Systems in batch, micro-batch, or in real-time as defined by TennCare SLA in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.6.3.1.7. The DQ/ETL Pipeline shall provide the tools for Data Source connectivity: adapters for a range of source types beyond Relational Database Management Systems (RDBMS's) and Legacy Databases (e.g. VSAM).

A.6.3.1.8. The DQ/ETL Pipeline shall load data in a variety of approaches including, but not limited to:

i) Bulk data extraction and loading;

ii) Granular trickle-feed acquisition and delivery;

iii) Changed-data capture (ability to identify and extract modified data);

iv) Event-based acquisition (time-based or data-value-based); and

v) Incremental data load per TennCare SLA in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.6.3.1.9. The DQ/ETL Pipeline shall support data transformation functions, including but not limited to:

i) Data-type conversion;

ii) Data reformatting;

iii) Data manipulation;

iv) String handling;

v) Lookups;

vi) Calculations; and

vii) Regular expressions.

A.6.3.1.10. The DQ/ETL Pipeline Contractor shall support application level role-based access to the DQ/ETL Pipeline to Create, Read, Update, and Delete (CRUD) in accordance with TennCare ITSM Policies and Procedures.

A.6.3.1.11. The DQ/ETL Pipeline shall have the ability to load all incoming source data in its original state and/or transformed data in the staging area/data lake (raw and cleansed).

A.6.3.1.12. The DQ/ETL Pipeline Contractor shall provide an ETL management tool that uses run-time monitoring, alerts, error handling, and logging.

A.6.3.1.13. The DQ/ETL Pipeline shall provide an exception handling mechanism such that the records that are identified as an error or exception can be processed separately.

A.6.3.1.14. The DQ/ETL Pipeline shall provide the ability to generate and manage notifications and alerts including how the alerts are registered, logged, and to whom the alerts are posted.

A.6.3.1.15. The DQ/ETL Pipeline shall provide reporting of results of an ETL session, including automatic notification of normal processing and failures of the ETL

process, description, and counts of exceptions. Notification types and recipients shall be agreed upon with TennCare during the design phase.

A.6.3.1.16. The DQ/ETL Pipeline shall provide the capability to schedule and monitor jobs/sessions.

A.6.3.1.17. The DQ/ETL Pipeline shall support the ability to recover from the abnormal ending of a transformation job and restart or rollback for a period defined by SLAs in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.6.3.1.18. The DQ/ETL Pipeline shall support concurrent processing of source data stream jobs (e.g. multiple, single) to improve performance when dealing with varied data volumes and usage.

A.6.3.1.19. The DQ/ETL Pipeline Contractor shall develop an ETL process with detailed mapping of data elements from Source Systems identified by TennCare to the target system's storage. The current representation of Source Systems is available in the Application and Interface Integration Inventory included in Attachment C, Procurement Library.

A.6.3.1.20. The DQ/ETL Pipeline workload shall not negatively affect the Source System, target system, EDW, or DSS in terms of performance or response times.

A.6.3.1.21. The DQ/ETL Pipeline shall provide environments with the automated capability to build and deploy source to target mappings for the corresponding target Data Model.

A.6.3.1.22. The DQ/ETL Pipeline shall be able to provide a one-time load (conversion) of data as approved by TennCare including, but not limited to, Data Sources identified in Attachment C, Procurement Library.

A.6.3.1.23. The DQ/ETL Pipeline shall have the ability to extract, transform, and load the data from disparate Data Sources for incremental data load and also for one-time load (conversion) per the TennCare Data Conversion/Management Plan.

A.6.3.1.24. The DQ/ETL Pipeline shall provide the capability to extract, transform, and load TennCare's current and future data volumes. See Attachment C, Procurement Library, for average data volumes that TennCare processes.

A.6.3.1.25. The DQ/ETL Pipeline shall execute data load (ETL, ELT (extract-load-transform), streaming data) on a TennCare-approved schedule.

A.6.3.1.26. The DQ/ETL Pipeline shall include technology to satisfy the performance requirements as specified in the SLAs in Attachment B, Service Level Agreement and Liquidated Damages for DQ/ETL, including, but not limited to, efficient data acquisition technology, high speed load utilities, and highly parallelized ETL processing.

A.6.3.1.27. The DQ/ETL Pipeline shall use the criteria/business rules defined by TennCare to create and manage the data load/ingestion configuration.

A.6.3.1.28. The DQ/ETL Pipeline shall record all failed transactions in tables/files. Transactions shall be retrievable for automated and manual processing.

A.6.3.1.29. The DQ/ETL Pipeline shall support automatic creation of primary keys (based on table definitions) in the target tables.

A.6.3.1.30. The DQ/ETL Pipeline shall provide the capability to perform data transformation, including but not limited to, partitioning, normalization, consolidation, derivation, and other structural data transformations.

A.6.3.1.31. The DQ/ETL Pipeline shall have the ability to apply selection criteria to aggregate, join and merge data, and calculate data fields.

A.6.3.1.32. The DQ/ETL Pipeline shall support user-defined SQL statements and other forms of scripting within the ETL tool.

A.6.3.1.33. The DQ/ETL Pipeline shall provide the capability to monitor, tune, and report the performance (e.g. data load time) of the extract, transform, and load processes.

A.6.3.1.34. The DQ/ETL Pipeline shall embed quality controls (e.g. CHECKSUM and number of rows read and processed) throughout the entire ETL process.

A.6.3.1.35. The DQ/ETL Pipeline shall have the ability to provide controls including, but not limited to:

i) Preventive controls (i.e. controls designed to prevent errors and unauthorized events from occurring);

ii) Detective controls (i.e. controls designed to identify errors and unauthorized transactions which have occurred in the system); and

iii) Corrective controls (controls to ensure the correction of Problems identified).

A.6.3.1.36. The DQ/ETL Pipeline shall support and maintain data integrity throughout the ETL processes.

A.6.3.1.37. The DQ/ETL Pipeline shall provide the capability to apply data mapping and transformation rules against source data.

A.6.3.1.38. The DQ/ETL Pipeline shall have ability to support standard-based technology agnostic APIs and micro services throughout the DQ and ETL processes.

A.6.3.1.39. The DQ/ETL Pipeline shall have the capability to make the T-MSIS extracts available to Enterprise-Wide TennCare applications through the ISL and other DE Components.

A.6.3.1.40. The DQ/ETL Pipeline Contractor shall ensure T-MSIS extracts are generated, validated, and approved with TennCare at least seven (7) calendar days prior to the monthly extract submission to CMS.

A.6.3.1.41. The DQ/ETL Pipeline shall have the capability to import or export data in a variety of formats (e.g.: CSV, XML, JSON) from/to other tools, database, and files.

A.6.3.1.42. The DQ/ETL Pipeline shall have the ability to capture Metadata and have the capability to import Metadata from or export Metadata in a variety of formats (e.g.: CSV, XML, JSON) from/to DE Components adhering to TennCare Data Policies and Standards.

A.6.4. Metadata Management

A.6.4.1.1. Metadata Repository

A.6.4.1.1.1. The DQ/ETL Pipeline Contractor shall maintain a Metadata Repository to contain all Metadata, PHI, PII, FTI, Confidential Information, or other such Sensitive Data, for the TennCare enterprise, as defined by TennCare. The Metadata Repository shall also contain, but is not limited to, Metadata derived from applications within the TennCare enterprise and Metadata derived from technical specification and design documents.

A.6.4.1.1.2. The DQ/ETL Pipeline Contractor shall maintain a Metadata Repository to add, view, update/maintain, and report versions of

Metadata (e.g. business, technical) from all sources as defined in the TennCare Data Policies and Standards.

A.6.4.1.1.3. The DQ/ETL Pipeline Contractor shall create an online accessible data catalog to store Metadata such as definitions of data elements and tables.

A.6.4.1.1.4. The DQ/ETL Pipeline Contractor shall include an online accessible data catalog with advanced, customizable, and complex search capabilities.

A.6.4.1.1.5. The DQ/ETL Pipeline Contractor shall support application-level, role-based access to the DQ/ETL Pipeline, based on security model, to add, view, edit/update, and logically delete Metadata, in accordance with TennCare ITSM Policies and Procedures.

A.6.4.1.1.6. The DQ/ETL Pipeline Contractor shall provide tools for enabling business and technical staff to locate and access Metadata for specific data elements using functionality such as a keyword search function, definitions appearing automatically when hovering the pointer over a data element, and the use of hot links from displays to the data definition.

A.6.4.1.1.7. The DQ/ETL Pipeline shall have the ability to track Data Sources, including the original source and changes of the source throughout the data lifecycle.

A.6.4.1.1.8. The DQ/ETL Pipeline shall comply with the XML Metadata Interchange (XMI) Standard.

A.6.4.1.1.9. The DQ/ETL Pipeline Contractor shall review and update Metadata for accuracy and completeness on a frequency defined by TennCare.

A.6.4.1.1.10. The DQ/ETL Pipeline shall have the capability to import Metadata from or export Metadata in a variety of formats (e.g.: CSV, XML, JSON) from/to other tools, consumers, and producers including, but not limited to, data analytics, reporting, or mining tools.

A.6.5. DQ/ETL Pipeline Administrative Requirements

A.6.5.1.1. Responsibilities

A.6.5.1.1.1. The DQ/ETL Pipeline Contractor shall ensure all Dashboards and reports adhere to all standards defined by TennCare for design and appearance during the design phase.

A.6.5.1.1.2. The DQ/ETL Pipeline Contractor shall create data extract and transfer information through the ISL to submit to T-MSIS in an acceptable format submitted to CMS and approved by TennCare.

A.6.5.1.1.3. The DQ/ETL Pipeline Contractor shall utilize TennCare's ITSM tools or include a workflow to manage all data requests and have the capability to integrate with TennCare workflow management tools, including, but not limited to IT Service and Change Management Tools.

A.6.5.1.1.4. The DQ/ETL Pipeline Contractor shall conduct requirement and design sessions with TennCare staff and stakeholders.

A.6.5.1.1.5. The DQ/ETL Pipeline Contractor shall work with TennCare and MMPVP to identify, define, integrate, and maintain all Data Sources deemed necessary to the DQ/ETL Pipeline. The DQ/ETL Pipeline Contractor is required to accommodate the types and numbers of Data Sources included in the TennCare Data Sources Service Type – Definitions and Scoring located in Attachment C, Procurement Library, throughout the

Contract term. The DQ/ETL Pipeline Contractor shall include all such identified Data Sources in the TennCare Data Sources Service Type – Definitions and Scoring as part of the DQ/ETL Pipeline at no additional cost to TennCare. For each unique Data Source after the allocated Data Source types and numbers included in the TennCare Data Sources Service Type – Definitions and Scoring are exhausted, integration will be authorized through the Change Order process in accordance with A.12.7.

A.6.5.1.1.6. The DQ/ETL Pipeline Contractor shall work with TennCare to retire Data Sources throughout the life of this contract, in consultation with TennCare. Data Sources identified for retirement shall adhere to the process outlined within the TennCare Project Change Management Standard included in Attachment C, Procurement Library.

A.6.5.1.2. Training

A.6.5.1.2.1. In addition to the training requirements in A.12.2, the DQ/ETL Pipeline Contractor shall develop and implement a written and customized train-the-trainer training plan for how to integrate with the ETL Pipeline Component functions.

A.6.5.1.2.2. The DQ/ETL Pipeline Contractor shall provide ongoing train-the-trainer sessions to address system or functionality changes for the DQ/ETL Pipeline as needed throughout the duration of the Contract.

A.7. Data Governance

A.7.1. The Contractor shall support internal policy and procedures to promote data documentation, development, and management of defined data entities, attributes, Data Models, and relationships sufficiently to convey the overall meaning and use of Medicaid data and information in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards.

A.7.2. The DE Component shall prevent unauthorized access, use, abuse, disclosure, disruption, or modification of data without proper TennCare consent.

A.7.3. The DE Component shall prevent unauthorized purging of data such that the data is no longer recoverable and useable in accordance with TennCare Data Policies and Standards.

A.7.4. The DE Component shall provide user-defined auditable events and corresponding audit logs for the access, use, abuse, disclosure, disruption, modification, deletion, and destruction of data.

A.7.5. The Contractor shall provide the capabilities necessary to implement the Data Steward processes as described in TennCare Data Policies and Standards, including but not limited to, review of Data Quality checks.

A.7.6. The Contractor shall ensure that the DE Component has the ability, at a minimum, to store, archive, retrieve, and purge data according to the TennCare Records Retention Policy and Records Disposition Authorization (RDA) List, and as defined by TennCare Data Policies and Standards or agreed upon by TennCare.

A.7.7. The DE Component shall retain all DE related application, network, system, and perimeter data including logs, files, and records for a minimum of ten (10) years or as defined by TennCare.

A.7.8. The Contractor shall maintain logs that are readily accessible to TennCare staff at no cost for one hundred eighty (180) days and retain in accordance with the TennCare Enterprise Security Policy, TennCare Data Policies and Standards, and TennCare Record Retention Policy in accordance with the SLAs in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.7.9. The Contractor shall support the adoption of Enterprise-Wide standard data definitions and data semantics in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards.

A.7.10. The Contractor shall ensure data integrity to validate key identifiers and ensure accuracy of data, including referential integrity, in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards.

A.7.11. The DE Component shall support tracking of Source Systems necessary for cataloging of Data Sources in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards.

A.7.12. The Contractor shall maintain compliance with the most recent TennCare Data Policies and Standards document, as it is periodically updated by TennCare. This ongoing compliance shall be performed at no additional cost to TennCare.

A.7.13. The DE Component shall have the ability to capture their respective components' business Metadata, technical Metadata, and all other Metadata as defined in TennCare Data Policies and Standards.

A.8. Hosting

A.8.1. Hosting Environment

A.8.1.1. Cloud Solution

A.8.1.1.1. The DE Component must be hosted in a public cloud-hosted environment.

A.8.1.1.2. The DE Component shall include all environments necessary to develop and test changes to the DE platform and to support the testing of the MMP in accordance with the TennCare Solution Implementation Lifecycle.

A.8.1.1.3. The Contractor shall work with TennCare and State of Tennessee Strategic Technology Solutions to determine the secure domain name system (DNS) solution including strategy, design, implementation, infrastructure, and ongoing maintenance that allows proper forwarding between the MMP and the State datacenter.

A.8.1.1.4. The Contractor shall determine the network and bandwidth requirements for the DE Component and work with the IS Contractor and the MMIS Module, as applicable, for the design and setup of network connectivity required between MMIS Modules and State datacenter in collaboration with and approved by TennCare.

A.8.1.1.5. The Contractor shall communicate in writing to TennCare the overall approach to hosting, including systems and operations under the auspices of subcontractors, at the request of TennCare.

A.8.1.1.6. If the DE Component is native to or currently implemented in a particular commercial cloud, the Contractor shall procure a dedicated cloud account for the TennCare DE Component, at no additional cost to TennCare. If the Contractor deploys to a State-owned Cloud offering, the Contractor shall assume all costs associated with the deployment and operations as part of the Maximum Liability to this Contract.

A.8.1.1.7. The Contractor shall provide TennCare with access and complete visibility into the TennCare DE Component dedicated cloud account. The Contractor shall generate reports to provide to TennCare on an as-needed basis that track the following, including, but not limited to, the usage and spending across projects, applications, and cost centers.

A.8.1.1.8. The Contractor shall create, based on TennCare review and approval, the organization structure and related cloud accounts for TennCare.

A.8.1.1.9. The Contractor shall identify Account Owners to create the administrators specific to the TennCare account.

A.8.1.1.10. The Contractor shall leverage Commercial Off-The-Shelf (COTS) software to deliver the DE Component as a Turn-key Solution and configure On-demand to scale for use by TennCare.

A.8.1.1.11. The Contractor shall provide TennCare with an itemized cost breakdown for each project component and phase in an approved TennCare-specified format, inclusive of ongoing cloud-related infrastructure costs, as applicable. The Contractor, as part of the Deliverable Payment process, shall detail the itemized costs during DDI and during O&M, in accordance with C.5 including, but not limited to:

A.8.1.1.11.1. Computing cost based on TennCare's cloud configuration by environment;

A.8.1.1.11.2. Network and telecommunication cost;

A.8.1.1.11.3. Data storage cost (active, infrequent, and archive) and data ingress-egress cost (in-transit); and

A.8.1.1.11.4. Transaction cost related to the number of reads, writes, and size of data packets.

A.8.1.1.12. The Contractor shall work with TennCare to agree on a patching schedule and frequency that meets the requirements defined in the Enterprise Information Security Policies (Section E.8.b.1);); exceptions to the agreed-upon schedule shall be approved by TennCare.

A.8.1.1.13. The DE Component shall support both DNS name-based whitelisting as well as IP based.

A.8.2. Business Continuity/Disaster Recovery

A.8.2.1. In the event of a Disaster, the Contractor, in coordination with TennCare, shall have the capability to determine that the primary production site is inoperable. Once a Disaster has been declared by TennCare, the Contractor shall initiate the Business Continuity/Disaster Recovery Plan (BC/DR) and move operations to the Disaster recovery site following the approved Disaster recovery plan in accordance with the TennCare SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL. The Contractor shall not return to the original production site without approval of TennCare.

A.8.2.2. The availability schedules and corresponding TennCare SLAs, defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, for the production environment shall apply to the Disaster recovery environment when fulfilling the production role.

A.8.2.3. The Contractor shall plan and coordinate Disaster recovery activities with the IS Contractor, MMPVPs, and TennCare partners to validate connectivity and interoperability for integrated applications.

A.8.2.4. The Contractor shall keep the BC/DR up-to-date and include recovery of any new functionality or integrations implemented during the previous year to the following year's annual Disaster recovery demonstration.

A.8.2.5. The Contractor shall coordinate with and demonstrate to TennCare the BC/DR every calendar year in conjunction with the annual testing demonstration in accordance with SLAs defined in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL. In the event the Contractor's test is deemed by TennCare to be unsuccessful, the

Contractor shall continue to perform the test until satisfactory results are received and approved by TennCare.

A.8.2.6. The Contractor shall execute a Disaster recovery test to demonstrate the Contractor's capability to restore processing capability in accordance with the BC/DR and for all critical system components at a remote site within twelve (12) months of Go-Live and every twelve (12) months thereafter. The BC/DR test shall be included as a part of operational readiness. The length of the test shall be the amount of time that is necessary to recover from the Disaster and provide proof that the recovery has been successfully completed. The Contractor shall work with TennCare to determine the DR test date at least one (1) month in advance and submit BC/DR plans for TennCare review at least fifteen (15) days prior to the DR test date. All findings and feedback provided by TennCare for the BC/DR plans must be resolved and approved prior to the Disaster Recovery test.

A.8.2.7. The Contractor shall maintain a BC/DR that provides for the recovery of critical services in accordance with SLAs defined in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, upon the discovery of a service disruption, the declaration of a Disaster, or if the production site becomes unsafe or inoperable.

A.8.2.8. The Contractor shall ensure that the BC/DR includes recovery of systems and operations under the auspices of subcontractors and adhere to the same TennCare SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.8.2.9. The Contractor shall implement a notification process approved by TennCare to notify contacts identified by TennCare in accordance with the BC/DR.

A.8.2.10. The Contractor shall ensure the BC/DR provides a framework for reconstructing vital operations to ensure the safety of employees and the resumption of time sensitive operations and services in the event of an emergency, provides for initial and ongoing notification procedures, and complies with all NIST 800 34 “Contingency Planning Guide for Federal Information Systems” standards.

A.8.2.11. The Contractor shall provide annual test reports to TennCare within five (5) Business Days of the exercise, BC/DR Plan reports within one (1) Business Day of incident, and BC/DR Plan updates within one (1) Business Day of an identified deficiency.

A.8.3. Backup and Restore

A.8.3.1. The Contractor shall design and implement backup and recovery measures that meet TennCare's backup and retention requirements in accordance with SLAs defined in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.8.3.2. The Contractor shall perform incremental and full backups of the DE Component in a secure location maintaining redundant copies of backups as needed to mitigate data loss, as defined in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.8.3.3. The Contractor shall be responsible for the backup, recovery and restoration of applications, Databases, files, and servers related to the DE Component.

A.9. Technical Requirements

A.9.1. Technology Standards

A.9.1.1. The Contractor shall ensure that the DE Component is able to handle current and future standards and requirements including, but not limited to: ICD-9 and ICD-10 including any future versions of ICDs, Health Insurance Portability and

Accountability Act (HIPAA), the Patient Protection and Affordable Care Act (PPACA), and the Health Information Technology for Economic and Clinical Health Act (HITECH).

A.9.1.2. The DE Component shall provide a flexible framework that allows the import and export of data using industry-standard file transmission protocols.

A.9.1.3. The DE Component shall have the ability to support the exchange of data or files via batches, web-services, queues, or other common message brokering protocols.

A.9.1.4. The Contractor shall comply with TennCare's Governance Framework as outlined in the TennCare IS Governance Standard included in Attachment C, Procurement Library.

A.9.1.5. The DE Component shall align with the CMS Medicaid Information Technology Architecture (MITA) framework.

A.9.1.6. The Contractor shall consult the TennCare Preferred Technology Standard in Attachment C, Procurement Library, and align the DE Component's technology, including the cloud environment, with TennCare's existing investment and technology preference. The Contractor may propose, and TennCare will consider, technology or tools using alternative products (e.g. cloud-native tools), if the technology or tools are equal or less than the cost of TennCare's preferred technology or tools, meets or exceeds all applicable requirements in this Contract, and aligns with TennCare's MMP objectives.

A.9.1.7. The DE Component shall comply with all HIPAA standard Transactions and Code Sets (TCS) as mandated by TennCare and CMS.

A.9.1.8. The DE Component shall comply with Industry Standards including, but not limited to, EDI/X12, NIEM, CAQH-CORE, HL7/FHIR, NCPDP, and HIPAA for data interchange.

A.9.1.9. The Contractor shall follow ITSM procedures to provide role-based access and integrate with the IAM solution through the IS Contractor to establish the appropriate use of the DE Component.

A.9.1.10. The DE Component shall display a query duration timer that will provide users with the total estimated time to run and the estimated time remaining for a query.

A.9.1.11. The Contractor shall, upon obtaining written authorization from TennCare, implement and support integration with existing TennCare enterprise tools for functions that include but are not limited to, File Integrity Monitoring (FIM), Security Operations Center (SOC), and Security Incident Event Management (SIEM). The Contractor shall identify the integration data points, thresholds, and/or format for TennCare's approval.

A.9.1.12. The Contractor shall implement and support integration for functions including, but not limited to, Problem resolution, incident management, and Event Management between the TennCare ITSM and the Contractor-managed security, governance, and monitoring tools. The tools shall include, but are not limited to, Network Operations Center (NOC), antivirus, vulnerability, software licensing, Governance Risk and Compliance (GRC), penetration testing, code scanning and quality Database auditing, cloud cost, backups, and CMS account transfer. The Contractor shall identify the integration data points, thresholds, reporting, frequency and/or format for TennCare's approval.

A.9.1.13. The Contractor shall plan and implement tools required for data transfer and ensure that data can be transferred from TennCare operational environments including MMP Modules to DE and within DE Components at no additional cost to TennCare.

A.9.1.14. The Contractor shall plan and implement tools required for data storage and ensure that data can be stored in active, infrequent, or archive storage spaces.

A.9.1.15. The Contractor shall plan and implement tools required for data archive and ensure that data can be archived and accessible at TennCare's request or as required for analytical purposes.

A.9.1.16. The Contractor shall plan and implement tools required to restore data from archive and ensure that data can be restored and accessible at TennCare's request.

A.9.1.17. The Contractor shall plan, estimate, and include all cloud-related costs including, but not limited to, compute, storage, data transfer, encryption, availability zones, multiple cloud architectures, TennCare and State of Tennessee Strategic Technology Solutions data center(s) integration, and any other cloud services. Such cloud services shall be included in the fixed price and shall not result in additional cost to TennCare or the State of Tennessee during the Contract term. Current TennCare data volumes and transaction volumes are provided in Attachment C, Procurement Library, for reference purposes.

A.9.2. Accessibility

A.9.2.1. The Contractor and DE Component shall comply with the Electronic and Information Technology accessibility requirements under the federal civil rights laws including Section 504 and Section 508 of the Rehabilitation Act of 1973 (Section 508) and the Americans with Disabilities Act (or any subsequent standard adopted by an oversight administrative body, including the Federal Accessibility Board). To comply with the accessibility requirements for Web content and non-Web electronic documents and software, the Contractor shall use the most current W3C's Web Content Accessibility Guidelines (WCAG) level AA or higher for the DE Component (For the W3C's guidelines see: https://www.w3.org/WAI/ and https://www.access-board.gov/guidelines-and-standards/communications-and-it). The Contractor's accessibility responsibilities shall include ensuring optimization of the DE Component by: integrating as appropriate the concept of transversality (the ability to transition from one webpage to another webpage with the understanding for where you are navigating to), which is inherent in Electronic and Information Technology accessibility; working with key individuals to plan accessibility at each step of the DE Component's design, development, implementation, and enhancement phases including testing and submitting evaluation reports to TennCare; appropriately allocating the accessibility project responsibilities; ensuring the accessibility technical and functional criteria are met at every milestone that contains an accessibility component for the DE Component; understanding the difference between accessible content and conforming content; being aware of the DE Component's testing tools and any limitations the tools have for testing accessibility and providing workarounds; and assessing the impact of technology platforms on the DE Component (i.e. applications, portals, and tools should work and be accessible across different platforms).

A.9.2.2. Contractor agrees to perform regularly scheduled (i.e., automatic) scans and manual testing for the most current WCAG level AA or higher compliance for all user content and applications in order to meet the standards for compliance. The Contractor must ensure that any system additions, updates, changes or modifications comply with the most current WCAG level AA or higher. COTS products may be used to verify aspects of the most current WCAG level AA or higher compliance.

A.9.2.3. The Contractor shall designate a staff member to be responsible for Contractor's Electronic and Information Technology accessibility compliance

activities to be performed under this Contract. The name and contact information for this individual shall be provided to TennCare's Office of Civil Rights Compliance (OCRC) within ten (10) days of the implementation phase of this Contract and within ten (10) days of this position being reassigned to another staff member, including reassignment due to vacancy.

A.9.2.4. Prior to the start of this Contract and on an annual basis thereafter, the Contractor's staff that is designated to work on the DE Component shall receive training on Electronic and Information Technology accessibility requirements. The Contractor shall be able to show documented proof that this training was provided. In addition, Contractor shall provide a copy of its Electronic and Information Technology accessibility training to TennCare's OCRC during the implementation phase of the Contract and upon request.

A.9.2.5. Should the DE Component or a component of the DE Component fail to comply with the accessibility standards, the Contractor shall develop and submit to TennCare for approval a noncompliance report that identifies the areas of noncompliance, a plan to bring the system or component into compliance, an alternative/work around that provides users with the equivalent access to the content, and a timeframe for achieving that compliance. TennCare shall review the noncompliance report to determine whether or not it is acceptable and should be implemented. Once the noncompliance report is approved by TennCare the Contractor may implement the compliance plan. TennCare, in its sole discretion, shall determine when a satisfactory compliance plan resolution has been reached and shall notify the Contractor of the approved resolution. If Contractor is unable to obtain content that conforms to the most current WCAG level AA or higher, it shall demonstrate through its reporting to TennCare that obtaining or providing accessible content would fundamentally alter the nature of its goods and services or would result in an undue burden.

A.9.2.6. The Contractor agrees to comply with Title VI of the Civil Rights Act of 1964. As part of achieving Title VI compliance, the Contractor should add a system function that allows users to translate the content into a language other than English. This requirement may be satisfied by the provision of a link to Google translate or other machine translate tool or translating the page into non-English languages as directed by TennCare and set forth in A.9.6.1.

A.9.2.7. The Contractor shall comply with the civil rights requirements set forth in 42 C.F.R. § 433.112 regarding the design, development, installation, or enhancement of mechanized processing and information retrieval systems. In addition, the Contractor shall participate in TennCare's effort to comply with the nondiscrimination requirements for acquiring automatic data and processing equipment and services set forth in 45 C.F.R. § 95.633.

A.9.3. Manageability/Reporting

A.9.3.1. The Contractor shall establish and manage a system diagnostics and monitoring tool in the DE Component to provide automatic system monitoring.

A.9.3.2. The DE Component shall detect, notify, and prevent run-away/long-running reports or queries that consume system resources, incur extra costs, and impact system operations.

A.9.3.3. The DE Component shall capture all statistics required to measure the contractual SLAs defined in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, and provide reports to TennCare at a frequency to be determined by TennCare or upon request, including, but not limited to

A.9.3.3.1. Number of transactions;

A.9.3.3.2. Response time;

A.9.3.3.3. Errors counts;

A.9.3.3.4. Types of transactions;

A.9.3.3.5. Incident response time; and

A.9.3.3.6. Number of incidents.

A.9.3.4. The DE Component shall provide detailed alerts and logging of all service failures and exceptions.

A.9.3.5. The Contractor shall document the high-level solution for the administrative functions of cataloging and monitoring all jobs and queries, inclusive of the approach and process in remediating jobs or queries.

A.9.3.6. The DE Component shall provide systematic notifications to identified users.

A.9.3.7. The DE Component shall include ongoing performance monitoring and remediation.

A.9.3.8. The DE Component shall allow users to view the status of scheduled, submitted, and canceled reports.

A.9.3.9. The Contractor shall provide configure and operate tools and a monitoring function to monitor key performance indicators (KPIs) metrics such as, but not limited to, response time, resource availability, CPU utilization, network load, memory utilization, application performance, end-user experience, and post-resolution analysis.

A.9.3.10. The Contractor shall provide TennCare access and complete visibility into the Contractor's tool(s) for reporting KPIs for validation by TennCare upon request.

A.9.3.11. The DE Component shall send alerts based on the monitored system attributes that are escalated through the Incident Management process documented in the Incident Management Plan.

A.9.3.12. The DE Component shall support monitoring, configuration of alerts, and configuration of notifications based on thresholds defined by TennCare.

A.9.3.13. The Contractor shall, if applicable, monitor, track, and report to TennCare infrastructure space and storage trends over the term of the Contract, including space and storage for staging and EDW Databases, MDM, DQ, and ETL.

A.9.3.14. The Contractor shall deliver all reporting and analytical requests on a TennCare-approved schedule.

A.9.3.15. The DE Component shall automate routine reports as required by TennCare on a daily, weekly, monthly, annual, and other frequencies. These routine reports will be generated and transported without manual intervention and include notifications to Authorized Users upon completion.

A.9.3.16. The DE Component shall provide a performance Dashboard(s), as approved by TennCare, of application services and network services providing the ability to drill down to a level where the observations provide useful information and both real-time and snapshot views. The Dashboard(s) shall allow authorized TennCare personnel to perform monitoring through graphical user interfaces.

A.9.4. Scalability

A.9.4.1. The DE Component shall be scalable and adaptable to meet future growth and expansion/contraction needs, such that the DE Component can be

expanded on demand and be able to retain its performance levels when adding additional users, functions, and storage.

A.9.4.2. The DE Component shall be scalable both horizontally and vertically to support the defined performance SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.9.4.3. The Contractor shall produce a capacity and performance plan approved by TennCare prior to any infrastructure build and as required by the TennCare Solution Implementation Lifecycle.

A.9.5. Availability

A.9.5.1. The DE Component shall be architected with no single point of failure, supporting fault tolerance and failover of application, database, servers, storage devices, and secondary devices such as load balancers, and supporting a high-availability enterprise.

A.9.5.2. The Contractor shall ensure average application-specific system response times are within application SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, excluding scheduled downtime, natural disasters, and force majeure, or as agreed to in the Contract.

A.9.5.3. The DE Component shall remain fully functional during backup windows.

A.9.5.4. The DE Component shall ensure information delivery in instances when systems or networks may go offline (e.g. Guaranteed Message Delivery, queuing of undelivered messages for reprocessing at a later time etc.).

A.9.5.5. The Contractor shall ensure that the production DQ/ETL Pipeline are available 99.9% of the time 24 hours a day, seven (7) days a week, including associated portals and interactions, excluding TennCare approved planned downtime. The DE Component is considered unavailable when any of the capabilities do not function as described in this Contract and attached documentation.

A.9.6. Graphical User Interface (GUI)

A.9.6.1. The DE Component shall support multiple languages and localization, as agreed upon with TennCare, for its user interface, modeling screens, websites, and development tools including compatibility with online translation tools (e.g. Google translate). At a minimum, the following languages shall be supported: English and Spanish.

A.9.6.2. If the DE Component is supported by user-access website, the Solution shall be accessible and shall be compatible with all mainstream browsers. Mainstream browsers are defined as any browser that has greater than three percent (3%) of the US browser market, or greater than three percent (3%) of the US mobile-browser market, as determined by https://gs.statcounter.com/browser-market-share/all/united-states-of-america or other source as determined by TennCare, among all versions of that browser within the last two (2) years across all supported operating systems. .

A.9.6.3. The DE Component that is accessible from the public internet (e.g. websites) shall make the site's privacy policy and terms of service available prior to authentication.

A.9.6.4. The DE Component shall facilitate Internet/Intranet accessible, browser-based web capabilities with no client component download(s) for all authorized end users.

A.9.6.5. The DE Component supported websites or content accessed via a Web Browser shall display a dismissible alert when being accessed by a browser type or browser version that is not fully supported.

A.9.6.6. All DE Component supported websites shall be accessible using, but not limited to, mobile devices, tablets, and PCs.

A.9.7. Supportability

A.9.7.1. The Contractor shall innovate, mature, and improve TennCare's analytical and reporting capabilities of the DE Component throughout the term of the Contract. The Contractor shall obtain TennCare approval prior to implementing any such changes.

A.9.7.2. The Contractor shall be a proactive participant and contribute to TennCare's Enterprise-Wide architecture, TennCare's technology management processes, and further the innovation and improvement of TennCare's analytical and reporting capabilities throughout the term of the Contract in addition to requirements in Section A.11.10.6, Continuous Improvement Process throughout the term of the Contract.

A.9.7.3. The Contractor shall ensure and demonstrate that the DE Component runs on software/hardware vendor supported release levels (N-1) at all times or (N-2) with exceptions/approval from TennCare.

A.9.7.3.1. The Contractor shall provide backward compatibility for DE Component service consumers; and

A.9.7.3.2. The Contractor shall support the IS Contractor with the discontinuation of service versions and coordination of MMPVP activities to mitigate service discontinuation impacts.

A.9.7.4. The DE Component shall be adequately flexible to keep up with changing technology and regulatory changes by, at a minimum, using standard-based technology agnostic APIs, micro services, ETL, Cloud integration, Data Models and storage, workflows, reporting and analytical engine, and container technologies.

A.9.7.5. The DE Component shall be upgradable and preserve Solution customizations or provide a TennCare-approved upgrade path.

A.9.7.6. The Contractor shall ensure each of the COTS or commercially supported components in the DE Component is supported by COTS vendors for the duration of the Contract, including the option years. If a DE Component becomes unsupported by the COTS vendors during the lifetime of the Contract, the Component shall be replaced at no additional expense to TennCare.

A.9.7.7. The Contractor shall enforce the enterprise Data Quality and governance policies and processes defined and approved by TennCare.

A.9.7.8. The Contractor is prohibited from leveraging the use of proprietary hardware, software, or other coding that might impede on TennCare's ability to support and maintain the environment.

A.9.8. Audit/Audit Support

A.9.8.1. The Contractor shall establish policies, procedures, and practices, in accordance with the requirements of this Contract, to ensure there is appropriate internal monitoring of the audit logs and the established process produces documentation to evidence the monitoring effort.

A.9.8.2. The DE Component shall support the capability for a centralized log of prescribed system events, and provide correlated logs, if the logs are

produced by multiple system Components, for ingestion by log aggregation software.

A.9.8.3. The DE Component shall ensure all incoming and outgoing transaction data is logged, archived in Human-Readable formats, and made reasonably available to support auditing, reporting, and other business needs in accordance with the SLAs in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.9.8.4. The Contractor shall implement Database auditing tool(s) as required by TennCare, State, and Federal regulations, and provide TennCare with the ability to review any and all audit data as applicable.

A.9.8.5. The DE Component shall maintain an audit trail of all actions related to data/content in accordance with the Enterprise Security Policy and TennCare System Security Plan (SSP) controls which include, but are not limited to:

A.9.8.5.1. Date and time data/content entered in the DE Component;

A.9.8.5.2. Any actions taken on the data/content; including the date and time of the edits/modification;

A.9.8.5.3. Record the user responsible for the changes; and

A.9.8.5.4. Record all user inquiries even if no action was taken by the user.

A.9.8.6. The Contractor shall support TennCare during all internal or external audits, reviews, and collaborations, such as CMS, PERM, T-MSIS, OIG, and MIC, which includes capturing and providing all data required to comply with such audits as defined by TennCare within the required time frames.

A.9.8.7. The Contractor shall make available to TennCare the results of any third-party audit conducted, including, but not limited to, the Service Organization Control (SOC) 2 and Network Organization Control (NOC), on the Contractor's organization services within the scope of this Contract.

A.10. Privacy and Security

A.10.1. The Contractor shall review and sign the current version of the Acceptable Use Policy (AUP) on a period agreed upon with TennCare as stipulated in the TennCare Information Security Program Plan (ISPP), TennCare Enterprise Security Policy (ESP), and BTC-Pol-AdmSec-200605-02: Acceptable Use Policy and Acknowledgement.

A.10.2. The Contractor must complete security and privacy training and submit summary compliance reports to the TennCare Privacy Officer in accordance with TennCare Privacy, Security, and Confidentiality Policy (PRIV-013) or as otherwise requested during the term of the Contract and during any renewal period. The Contractor will be responsible for employees that support the TN Data Ecosystem being compliant on required security and privacy training. The Contractor must provide copies of all "table of contents" for security and privacy training materials upon request by TennCare. In the event of an audit or investigation, Contractor will provide detailed information including training completion records, if requested.

A.10.3. The DE Component shall provide security that is consistent with the requirements of this Contract and with the standards established by the IS Contractor for all Modules.

A.10.4. The Contractor shall be responsible for establishing, controlling, maintaining, and ensuring data privacy and information security program for the DE Component in coordination with the TennCare Security and Privacy Offices. These responsibilities include oversight of physical, technical, administrative, and organizational safeguards in accordance with, TennCare IT data security policies and plans,

including, where appropriate and at a minimum, the TennCare Data Privacy Program Policy and Plan, TennCare Enterprise Security Policy, and TennCare ISPP located in Attachment C, Procurement Library.

A.10.5. The Contractor shall provide and maintain a secure environment(s) that ensures confidentiality of all State records and other Confidential Information regardless of media or locations.

A.10.6. The Contractor shall design, document, develop, implement, operate, and maintain security controls over access to Sensitive Data (e.g. PII, PHI, FTI, etc.) from various sources as defined in the State and Federal policies and regulations according to the TennCare System Security Plan (SSP) Template and IRS Pub 1075. The SSP shall be delivered in a format as defined by TennCare or directly entered by the Contractor into the TennCare Governance, Risk, and Compliance (GRC) system.

A.10.7. The Contractor shall comply with any applicable State and Federal confidentially requirements regarding the collection, maintenance, use, and the protection from data loss, of health, personally identifiable, and financial information (PHI, PII, FTI, etc.). This includes, where appropriate and at a minimum, the latest guidance from Minimum Accept Risk Standards for Exchanges (MARS-E), Federal Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d, and IRS Publication 1075. Cloud infrastructure for TennCare systems containing FTI are required to be certified FedRAMP Moderate using FIPS-199 standards.

A.10.8. The Contractor shall meet all TennCare and Federal regulations regarding standards for privacy, security, and Protected Health Information (PHI).The Contractor shall maintain and operate the DE Component consistent with HIPAA and HITECH.

A.10.9. The Contractor shall employ a risk management framework in accordance with TennCare and Federal (NIST SP 800-37) security requirements.

A.10.10. The Contractor shall ensure all appropriate measures are in place for minimal use and protection per applicable regulations for the data types and classifications. Policies, procedures, and related controls around the use of Sensitive Data and segregation of duties shall be maintained and made reasonably available for review by TennCare.

A.10.11. The Contractor shall develop written policies, procedures, and standards of conduct to comply with all applicable TennCare and Federal standards for the prevention, detection, and reporting of incidents of potentially suspicious or questionable activity, fraud, and abuse by Members, providers, subcontractors, the Contractor, or external entities.

A.10.12. The DE Component shall align with and comply with all HIPAA Privacy, HITECH, and any applicable Security Compliance Regulations and Guidelines to protect and secure healthcare data. The Contractor shall acknowledge its obligation to adhere to Federal, State, and TennCare security requirements and to receive TennCare's approval of its Security Plan.

A.10.13. The Contractor shall be responsible for identifying and notifying TennCare of any Sensitive Data being stored, processed, viewed, or otherwise used by Contractor’s employees that does not comply with TennCare security and privacy policies and report in accordance to reporting requirements stipulated in TennCare’s Acceptable Use Policy (AUP) and TennCare Enterprise Security Policy.

A.10.14. The DE Component shall meet password-based authentication and identify requirements in accordance with NIST 800-63-3 and TennCare Enterprise Security Policy.

A.10.15. The Contractor shall implement alternative password reset capabilities in DE in accordance with TennCare Enterprise Security Policy, NIST guidelines, and industry best practices.

A.10.16. If the Contractor has a Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) Certification applicable to the Services and/or applications in scope for the Contract and maintains such certification throughout the period of the Contract, then that HITRUST certification covering the DE Component may be used in whole or part of the System Security Plan at TennCare's discretion when it meets Federal requirements to do so. To the extent the Contractor does not have HITRUST CSF certification prior to the start of the Contract, it must initiate the certification process within ninety (90) days of the start of the Contract and obtain and provide to TennCare such Certification within twenty-four (24) months of the start of the Contract. Other major industry- standard certifications with appropriate coverage and validation may be accepted at TennCare's discretion.

A.10.17. The DE Component and infrastructure shall adhere to best practices and use open security standards and frameworks, as appropriate, such as but not limited to:

A.10.17.1. Federation: WS-Secure Conversation, WS-Federation, WS-Authorization, XML Key Management (XKMS);

A.10.17.2. Mechanism: Extensible Access Control Markup Language (XACML), XML Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML), X.509 certificates; and

A.10.17.3. Policy: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL).

A.10.18. The DE Component shall implement a security architecture based on cloud security best practices, including but not limited to, NIST SP 800-550-292 Cloud Computing Reference Architecture and architectures referenced in the current Medicaid Information Technology Architecture (MITA) Security and Privacy model.

A.10.19. The Contractor shall coordinate with the cloud-service provider to implement and configure a compliant cloud architecture solution based on the Shared Responsibility Model to ensure all modules, data, and components are protected. The cloud solution shall be in compliance with NIST SP 800-53 Moderate, MARS-E Moderate, and other TennCare policies and guidance. The Contractor's cloud solution shall incorporate security best practices towards boundary protection, network segmentation, and access segmentation to include, where applicable and at a minimum, the implementation and configuration of Industry Standard Virtual Private Cloud (VPC), network and application firewalls (Next Generation Firewall (NGFW), Web Application Firewall (WAF)), security groups, subnets, network and data encryption, end-point protection (Antivirus (AV), Endpoint Detection and Response (EDR)), and Intrusion Detection and Prevention System (IDPS)) and shall be approved by TennCare during design.

A.10.20. The Contractor shall perform the installation, operations, and management of hardware, application, and operating system level hardening and secure configuration on the applicable DE Component platform and in accordance to the Design and Test Phases of the SILC, by TennCare and Federal hardening, and Configuration Management standards such as the TennCare Enterprise Security Policy, CIS Level 1, and FedRAMP appropriate guidelines.

A.10.21. The Contractor shall adhere to Database security in accordance with TennCare and Federal requirements for all data at rest and in motion.

A.10.22. The Contractor must ensure that the supply chain communicates, coordinates, and monitors Sensitive Data across the MMIS Modules and MMPVP integrations according to NIST SP 800-161, TennCare ISPP, and industry best practices.

A.10.23. The Contractor shall mask any Sensitive Data from the production environment for use in non-production environments unless the data owner pre-authorizes the use of Sensitive Data in the non-production environment.

A.10.24. The Contractor shall use synthetic data (secure, realistic, meaningful sets of data) for non-production activities. The IRS considers masked, derived, obfuscated, and de-identified data based on FTI to still be FTI. FTI in non-production environments must pass the IRS approval process.

A.10.25. The Contractor's data management strategy and operational policies and procedures shall meet HIPAA, HITECH, American Recovery and Reinvestment Act of 2009 (ARRA), TennCare policies and procedures, and requirements defined by State and Federal law for data classifications in use.

A.10.26. The DE shall utilize appropriate standards, protocols, and methodologies to restrict access to the system (in a manner acceptable to TennCare) when anomalies are identified or detected.

A.10.27. The Contractor shall ensure data loss prevention and Data Mining activities are audited and captured and implement all Access Controls (AC) in the NIST 800-53, MARS-E, and TennCare security and privacy guidelines.

A.10.28. The DE Component shall run from a service account with the least privilege. The DE Component shall not run from a system-level account with unlimited privileges such as "root" or "administrator".

A.10.29. The DE Component shall have the automated capability to support role-based access, to terminate access and generate alerts for conditions which violate security rules, unauthorized attempts to access data and system functions, and system activity based on security parameters per TennCare and Federal standards.

A.10.30. The DE Component shall integrate with the IAM/Single Sign-On (SSO) and provide a mechanism for Multi-Factor Authentication (MFA) and Step-up Authentication.

A.10.31. The Contractor shall establish applicable secure connection mechanisms, such as Virtual Private Network (VPN), Virtual Private Cloud (VPC)-peering, or using Transport Layer Security (TLS) standards, to access the DE Component in accordance to the TennCare Enterprise Security Policy, NIST Guidelines, FIPS 140-2, and newer standards.

A.10.32. The Contractor shall establish and manage cryptographic keys employed within the DE for key generation, distribution, storage, access, and destruction in accordance with TennCare and Federal guidelines to include but not limited to NIST SP 800-175 and FIPS 140-2 or newer standards.

A.10.33. The DE Component shall meet federal processing standards for encryption in storage and in transmission according to TennCare and FIPS 140-2, or newer standards.

A.10.34. The DE Component shall provide a central repository and management platform for security certificates and server host keys.

A.10.35. The Contractor shall encrypt data processed by the DE Component being stored, transmitted, or transported either physically or electronically as required by TennCare policy, State or Federal regulations, and industry-accepted encryption standards.

A.10.36. The Contractor shall encrypt Confidential State Data at rest and in transit using the most recent version of Federal Information Processing Standard (“FIPS”) 140-2 validated encryption technologies.

A.10.37. The Contractor shall ensure that TennCare data is always transmitted and stored within secured cloud regions and zones that are within the continental United States (CONUS).

A.10.38. The DE Component shall provide full redundancy and recovery to ensure uninterrupted access to the certificates and keys.

A.10.39. The Contractor shall implement a code analysis process in accordance with TennCare Enterprise Security Policy.

A.10.40. The Contractor shall review security and application logs on a regular interval approved by TennCare to identify suspicious or questionable activity, including user fraud and abuse cases, for investigation and documentation as to their cause and remediation. TennCare authorized security personnel or appropriate 3rd party assessor shall have the right to inspect security operations policies and procedures and the Contractor's performance to confirm the effectiveness of these measures for the Services being provided in support of regular audits.

A.10.41. The Contractor shall implement and manage appropriate technical security controls and safeguards to prevent the unauthorized access to, use of, or tampering with computers or computer systems, including hacker attacks, insider threat attacks, Advanced Persistent Threat (APT), abuse, and fraud, arising from the introduction of any form of malicious software including computer viruses, Trojans, worms, or otherwise causing damage to the Contractor's DE, TennCare, or third person's computer, computer system, network, or similar computer-related property and the data, software, and all programs.

A.10.42. The Contractor shall coordinate with TennCare to perform security vulnerability scanning and reporting on the DE Component and report results through the TennCare ITSM, to include APIs in accordance with TennCare's Enterprise Security Policy.

A.10.43. The Contractor shall conduct cyber threat analysis against the cloud DE Component, develop security monitoring use cases, (hereinafter referred to as "use case" or "use cases"), integrating a standard framework such as MITRE ATT&CK (PRE-ATT&CK, Mobile, and Enterprise), implement appropriate security analytics to detect and respond to potential threats, and test use case efficacy on a quarterly basis.

A.10.44. The Contractor shall have the ability to detect and monitor for security and privacy incidents, detect configuration weaknesses, vulnerabilities open to exploitation, and integrate relevant threat intelligence, including externally and internally derived indicators of compromise (IOCs) information, 24 hours, 7 days a week, 365-days a year (24x7x365).

A.10.45. In the event of a breach that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of the DE Component, the Contractor shall collaborate with TennCare and MMPVPs to respond to and triage the event in accordance with the Contractor's Incident Response Plan (IRP), the TennCare Enterprise Security Policy, and industry best practices. TennCare shall be notified of any incident or breach of TennCare in accordance with Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.10.46. The DE Component shall manage and adopt the Open Web Application Security Project (OWASP) Top 10 web security recommendations.

A.10.47. The Contractor shall provide and review with TennCare on an interval defined and approved by TennCare a use case usage report.

A.10.48. If applicable, the Contractor shall coordinate with the TennCare Cloud Access Security Broker (CASB) vendor and TennCare to integrate CASB capabilities to ensure TennCare security policies are enforced and in-synch between on-premise and/or cloud systems as it pertains to the DE Component.

A.10.49. The Contractor shall provide TennCare and Federal regulators the raw, un-redacted results of vulnerability scans, compliance scans, code scans, and any penetration test on demand.

A.10.50. The Contractor shall co-manage with TennCare the implementation of a TennCare-owned File Integrity Management (FIM) solution to include the following:

A.10.50.1. Install FIM agents across all servers used for the solution supporting TennCare;

A.10.50.2. Provide infrastructure to install FIM collectors in the same network as the DE;

A.10.50.3. Implement capabilities and setup network connectivity to synchronize FIM reports from collector servers to TennCare's centralized FIM; and

A.10.50.4. The Contractor is responsible for ensuring the agent's and the collector server's availability meets the SLAs defined in Contractor Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.10.51. All State owned/supported workstations shall be managed by STS using established State-standard software tools.

A.10.52. The Contractor shall install and configure TennCare-approved antivirus solutions across all servers used for the DE and make the findings available in a format and frequency as requested by TennCare.

A.10.53. The Contractor shall configure, implement, operate, and manage, as appropriate and approved by TennCare, the following endpoint protection capabilities to include, but not limited to:

A.10.53.1. Antivirus and antispyware;

A.10.53.2. Host firewall;

A.10.53.3. Host intrusion prevention system;

A.10.53.4. Host integrity check; and

A.10.53.5. Application device control.

A.10.54. The Contractor shall configure and develop endpoint protection security enforcement rules/policies, and other similar measures and schedule scans to continuously protect the DE Component from, but not limited to, anti-malware, ransomware, persistent threat, and data-loss attack activities monitored in real-time.

A.10.55. The Contractor shall provide TennCare with all endpoint protection security enforcement rules (e.g. events monitored, activity type) annually. This information will be contained within the System Security Plan (SSP).

A.10.56. The Contractor shall ensure that the endpoint security posture is in accordance to control requirements stipulated in the TennCare Enterprise Security Policy and security best practices.

A.10.57. The Contractor shall enable appropriate logging mechanisms on systems and applications to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events in accordance with information security standards, including TennCare ISPP and TennCare Enterprise Security Policy.

A.10.58. The DE Component shall utilize a Security Information and Event Management (SIEM) solution in accordance to the IRS SIEM tool standards found in the www.irs.gov Safeguards Program portal, Configuration Technical Assistance section. This standard is to be used as a best practice standard of implementing a SIEM for all data classifications.

A.10.59. The Contractor shall provide cloud security monitoring and detection capabilities, respond to security alerts in real-time, and work with TennCare towards security recovery actions.

A.10.60. The Contractor shall be responsible for implementing audit mechanisms to generate findings and reports across different layers of the DE Component (OS, application, system, data) in accordance with the TennCare Enterprise Security Policy, FedRAMP, and MARS-E Moderate level controls.

A.10.61. The Contractor shall ensure, cooperate, and coordinate with TennCare, to configure reliable, secure log data and event collection mechanisms, to include remote log data and event collection agents on machines, from various sources to forward and securely deliver the log data and event collection to TennCare for indexing and analysis. This includes the end-to-end process from log data collection, event generation, transmission, storage, and disposal.

A.10.62. The DE Component shall retain system audit and event logs and related data per retention requirements and in a format and structure that is approved by TennCare.

A.10.63. The Contractor shall retain and provide to TennCare security, system, and application logs in a format approved by TennCare.

A.10.64. The Contractor shall provide TennCare access to DE log data and events 24-hours a day, 7 days a week, 365 days a year (24x7x365). The DE shall be capable of creating a digital, reusable copy of TennCare's data, in whole and in parts in common and current machine-readable files. The Contractor shall enable TennCare to extract data from the DE on demand, but no later than within 24-hours of TennCare's request, at no additional cost to TennCare and without any conditions or contingencies.

A.10.65. The Contractor shall participate in audit activities and assist TennCare to prepare documentation required by TennCare and/or any regulatory bodies.

A.10.66. The Contractor shall have an annual audit performed by a qualified, third-party, independent audit firm ("Assessor") to conduct an assessment of the security and privacy controls in the DE Component and maintain the integrity of the audit process. A Security Assessment Plan (SAP) must be jointly completed and agreed to before the start of the assessment by all parties involved, including the Contractor, Assessor, and TennCare. The Assessor will use the methodology described in the template provided by TennCare to perform the assessment. A completed SAP must be submitted to TennCare seventy (70) days prior to the security assessment report kick-off date. The full un-redacted third-party independent assessment must be delivered to TennCare on demand within ten (10) Business Days upon receipt of the report from the third-party to share with State or Federal regulators.

A.10.67. The Contractor and TennCare shall mutually agree with the methodology and scope of the assessment prior to the commencement of the third-party independent audit of the DE Solution. If the Parties are unable to mutually agree, TennCare, in its sole discretion, may define the methodology and scope of the third-party independent audit. The Contractor shall provide evidence to validate all security, privacy, and encryption requirements are met by providing TennCare access to all sourced evidence, such as but not limited to, firewall rules, vulnerability assessment reports, and code analysis reports. The Contractor shall provide TennCare with written evidence of findings (Defects, vulnerabilities, errors, gaps, weaknesses, or omissions) and their planned remediation in a Plan of Action and Milestones (POA&M), maintained monthly, until all findings are resolved and promptly modify its security measures in order to meet its obligations.

A.10.68. The Contractor shall provide TennCare with all search queries, search correlations, rules, alert definitions, and/or use cases at the request of TennCare.

A.10.69. The Contractor must create compliance and regulatory reports about security-related events and incidents, to include active use case test results as specified by TennCare.

A.10.70. The DE shall provide a Security Summary report and POA&M in accordance with TennCare's ISPP.

A.10.71. The Contractor shall report in a timely manner audit and risk assessments conducted directly by TennCare or indirectly by a party acting on TennCare's behalf for conducting reviews or assessments.

A.10.72. The Contractor shall ensure tracking of all change management and request activities beginning with pre-production, on all production systems and shall provide audit reports for tracking users, associated security groups, roles, settings, passwords and duplicate IDs. The frequency and content of security audit reports, to include TennCare ITSM Change State Model and Change Request reports (CRQ), will be determined by TennCare.

A.10.73. The DE Component shall track disclosures of PHI and PII and provide Authorized Users access to and reports on the disclosures. As part of the TennCare SSP Template, the HIPAA disclosure report shall be provided to TennCare within the time limits mandated per TennCare Privacy Program Policy and Plan (PRIV-028).

A.10.74. The Contractor shall respond to weaknesses identified and tracked in a POA&M captured as part of a periodic risk assessment against the DE. A POA&M must be developed and submitted to TennCare in accordance with TennCare's Enterprise Security Policy and the SSP process. The Contractor shall enter updates for remediation actions and milestones in TennCare's electronic Governance, Risk, and Compliance System. Additionally, the Contractor will be required to attend monthly meetings with TennCare security regarding POA&M's status.

A.10.75. The Contractor shall develop, maintain, and test an Incident Response Plan (IRP) with key partner roles both internal and external on an annual basis in accordance to the NIST SP 800-61 Revision 2 guidelines and TennCare Enterprise Security Policy to comply with all applicable Federal and State breach notification laws. Incident response roles and responsibilities must be clearly outlined and a RACI developed between the Cloud Service Provider (CSP), TennCare, Contractor, and Subcontractor, as appropriate, in event and security incident triage, analysis, containment, mitigation, response, and recovery.

A.10.76. The Contractor shall notify the TennCare Security and Privacy Offices within ten (10) Business Days of any solution or operational enhancements, Change Memorandums, or material changes agreed to with TennCare for all work product/work scope and required key Deliverables related to Security and Privacy development cycles. The notification shall be provided in a written email format to the TennCare Security and Privacy Offices.

A.10.77. The Contractor shall be responsible for the continuity of all security and privacy protocols for all solution or operational enhancements, Change Memorandums, or material changes agreed to with TennCare that are performed under this Contract, which develops a new system or significant change/enhancement to an existing system. The Contractor shall notify by written email to the TennCare Security and Privacy Offices upon agreement of solution or operational enhancements, Change Memorandums, or materials changes.

A.10.78. The DE Component shall utilize the TennCare-provided IAM solution and shall provide Role-Based Security for the identity management and authentication of end-users of this application. Changes or upgrades made to the IAM service constitute a change to all applications or services that utilize IAM. As with any change to an application or service, an IAM change will require appropriate testing and may require system changes to accommodate the IAM change.

A.11. Solution Implementation Lifecycle (SILC) Requirements

A.11.1. The Contractor shall follow TennCare's SILC as described in the TennCare Solution Implementation Lifecycle Standard located in Attachment C, Procurement Library. The TennCare Solution Implementation Lifecycle (SILC) defines TennCare's standard phased approach to solution implementation projects, details the TennCare Gate Review Process, outlines the requirement entry and exit criteria, and aligns the associated Deliverable for each Gate in the lifecycle for contractors partnering with TennCare.

A.11.2. The Contractor shall complete the required Deliverables as described in the TennCare Solution Implementation Lifecycle and defined in the DE TennCare

Solution Implementation Lifecycle RACI and Deliverables located in Attachment C, Procurement Library. The DE TennCare Solution Implementation Lifecycle RACI and Deliverables defines the activities and Deliverables the Contractor is required to submit to TennCare for approval in order to pass the associated Gate Review.

A.11.3. The Contractor shall integrate the approved project schedule within the Integrated Master Schedule managed by the Strategic Project Management Office (SPMO) in accordance with the TennCare Project Management Plan Standard located in Attachment C, Procurement Library.

A.11.4. Design, Development, and Implementation (DDI) Phase

A.11.4.1. The Contractor shall complete the activities and Deliverables assigned to "DE Component" in the "DDI DE Component Vendor" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for the DDI of the DE Component. The Contractor shall coordinate with the EDW Contractor, as applicable, to prioritize and complete the activities and Deliverables in the SILC RACI.

A.11.4.1.1. The EDW Contractor shall complete the activities and Deliverables assigned to "EDW Vendor" in the "DDI EDW Vendor" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for the DDI of the EDW.

A.11.4.1.2. The EDW Contractor shall be responsible for completing all system integration activities across DE Components.

A.11.4.2. All required Deliverables must be submitted to TennCare and approved according to the Deliverable's Business Review Cycle defined in the "Deliverable Definition" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables. If the Deliverable does not have a defined Business Review Cycle in column H of the "Deliverable Definition" tab, TennCare shall designate each Deliverable(s) classification at the start of the phase in which the Deliverable is to be completed.

A.11.5. Operations & Maintenance (O&M) Phase

A.11.5.1. The Contractor shall complete the activities and Deliverables assigned to "DE Component" in the "O&M DE Component Vendor" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for O&M of the DE Component. The Contractor shall coordinate with the EDW Contractor, as applicable, to prioritize and complete the activities and Deliverables in the SILC RACI.

A.11.5.1.1. The EDW Contractor shall complete the activities and Deliverables assigned to "EDW Vendor" in the "O&M EDW Vendor" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for the O&M of the EDW.

A.11.5.2. All required Deliverables must be submitted to TennCare and approved according to the Deliverable's Review Cycle defined in the "Deliverable Definition" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables. If the Deliverable does not have a defined Review Cycle in column H of the "Deliverable Definition" tab, TennCare shall designate each Deliverable(s) classification at the start of the phase in which the Deliverable is to be completed.

A.11.5.3. In addition to the Deliverables identified in the TennCare Solution Implementation Lifecycle, the Contractor is responsible for activities defined in

the TennCare IT Service Management Standard located in Attachment C, Procurement Library.

A.11.5.4. The Contractor shall use an Information Technology Infrastructure Library (ITIL)-based approach for the development of all DE Component processes, procedures, and Deliverables.

A.11.6. Project Document Management

A.11.6.1. The Contractor shall store project documents in an online document library identified by TennCare. Project documentation includes, but is not limited to, Deliverables, Artifacts, work plan, status reports, status meeting agenda, and minutes.

A.11.6.2. The Contractor shall provide an electronic documentation format that facilitates efficient, effective, and expedited updating and dissemination of new or modified data.

A.11.6.3. The Contractor shall provide, at a minimum, a process to update the electronic versions of project documentation. Each version shall have:

A.11.6.3.1. All pages numbered within each section;

A.11.6.3.2. A new revision date on each page; and

A.11.6.3.3. All revisions clearly identified.

A.11.6.4. The Contractor shall provide a search capability with context-sensitive help screens within the project document library.

A.11.6.5. The Contractor shall provide online hyperlinks with references to Medicaid and non-Medicaid policy origination documents managed by TennCare and the Contractor within the project document library.

A.11.6.6. The Contractor shall adhere to the principle of least privileges and limit access to documentation that contains specific IP addresses, server names, node IDs, or other technical information that could compromise the security of the solution, to the level required for performance of necessary activities.

A.11.6.7. The Contractor shall categorize documentation by data classification, as defined by TennCare, and securely store sensitive technical documentation as approved by TennCare.

A.11.6.8. The Contractor shall include a reference to Tennessee Code Annotated (TCA) §10-7-504 where appropriate for sensitive and confidential technical documentation.

A.11.7. Deliverable Management

A.11.7.1. The Contractor shall adhere to all Quality Management Standards provided in TennCare's Project Management Plan Standard.

A.11.7.2. The Contractor shall ensure that documentation does not contain any protected Sensitive Data.

A.11.7.3. The Contractor shall handle identified Deliverables that require ad hoc updates or are updated periodically during the course of the implementation as follows:

A.11.7.3.1. The Contractor shall update content in the original Deliverable. Updated content provided in a deliverable amendment, and not integrated into the original deliverable, requires prior authorization by TennCare.

A.11.7.3.2. The Contractor's completion of, and TennCare's Acceptance of, a Deliverable during one (1) Gate Review shall be subject to the

approval of TennCare and shall not constitute Acceptance of that Deliverable by TennCare for any subsequent Gate Review.

A.11.7.4. At a minimum, the Contractor shall submit a Deliverable Expectation Document (DED) to TennCare for each Deliverable at least twenty (20) Business Days prior to the first submission date or a timeline approved by TennCare.

A.11.7.5. The Contractor shall create Deliverables as defined in each approved Deliverable's DED.

A.11.7.6. The Contractor shall facilitate, for each Deliverable, a minimum of one (1) walkthrough with TennCare and MMPVP one (1) week prior to the deliverable submission date or on a TennCare approved timeline.

A.11.7.7. The Contractor shall submit, for each Deliverable, a first submission on the agreed submission date, and the Contractor shall allow TennCare to review and provide responses.

A.11.7.8. The Contractor shall submit, for each Deliverable, a subsequent submission, as specified in Table 1: Deliverable Review Cycles, resolving comments received from TennCare on the previous submission and allowing TennCare to review and provide responses based on the project schedule.

A.11.7.9. The Contractor shall resolve all outstanding responses from TennCare prior to each Deliverable's final submission based on the project schedule.

A.11.7.10. The Contractor shall establish and maintain data integration, exchange, and interface documentation in alignment with TennCare Enterprise Architecture Framework Standard located in Attachment C, Procurement Library.

A.11.7.11. The Contractor shall follow the review and response times based on the complexity level bucket assigned to the Deliverable in the Table of Deliverables (Section A.13), as follows:

TABLE 1: DELIVERABLE REVIEW CYCLES

Deliverable Classification	Length of State Review Period for each Review Cycle	Length of Contractor Update Period after Receiving State Updates
Type A	Seven (7) Business Days	Seven (7) Business Days
Type B	Ten (10) Business Days	Ten (10) Business Days
Type C	Twenty (20) Business Days	Twenty (20) Business Days
Type D	Forty-Five (45) Business Days	Forty-Five (45) Business Days

A.11.8. Integration Services

A.11.8.1. The Contractor shall integrate the DE Component with TennCare's IAM solution.

A.11.8.2. The Contractor shall be solely responsible for obtaining, maintaining, and renewing all permits, approvals, licenses, certifications, and similar authorizations, including, but not limited to SSA certification, FedRAMP certification, CMS Certification, as required by any local, State, or Federal entities for the DE Component throughout the duration of the Contract.

A.11.8.3. The Contractor shall interface with the ISL, MMPVP Modules, and the individual DE Components using Industry Standard protocols and formats.

A.11.8.4. The Contractor shall be responsible for adherence to the established TennCare Integration Standards during implementation of the DE Component interfaces with MMPVPs.

A.11.8.4.1. The Contractor shall support TennCare and MMPVPs during the design, development, and implementation of integrations and interfaces of each of the MMIS Modules.

A.11.8.5. The Contractor shall develop appropriate architectural models of the solution design, selected with TennCare's approval, modeled in accordance with the TennCare Enterprise Architecture Modeling Standard, prior to the Solution Architecture Review. The Contractor shall load all Artifacts into the TennCare architecture repository tool, Sparx Enterprise Architecture.

A.11.8.5.1. If there are significant changes made to the architecture before Go-Live, the Contractor shall update the solution design models and present them for an As-Built Review, in accordance with the TennCare Enterprise Architecture Framework Standard.

A.11.9. Test Management

A.11.9.1. The Contractor shall ensure testing meets TennCare's functional requirements and non-functional requirements, including integration with other TennCare systems.

A.11.9.2. The Contractor shall adhere to the TennCare Test Management Standard in Attachment C, Procurement Library, for testing the development of a new solution and for testing the customization and integration of commercial software.

A.11.9.2.1. The Contractor shall collaborate with MMPVPs to plan, prepare for, execute, and report on testing;

A.11.9.2.2. The Contractor shall prepare a Test Management Plan for the DE Component and ensure that TennCare approves the proposed testing methods, schedule, personnel, training, collaboration approach, test cases, data, environment, tools, tracking, metrics, and methods for Defect management and regression testing;

A.11.9.2.3. The Contractor shall receive written authorization from TennCare for the use of real data for testing;

A.11.9.2.4. The Contractor shall be responsible for five (5) stages of testing before Go-Live and must provide evidence of their completion in the following Deliverables:

i. Unit Test Report;

ii. System Integration Test Report;

iii. User Acceptance Test UAT Report;

iv. Operational Readiness Test Report; and

v. Beta Test Report (as required by TennCare).

A.11.9.2.5. The Contractor shall test in the O&M and Retire phases based on the activities in the Test Standard Management Addendum.

A.11.9.2.6. The Contractor shall perform Regression Testing based on solution or other system changes.

A.11.9.2.7. The Contractor shall coordinate with the other DE Component Contractor(s), if any, and MMPVP to ensure the appropriate resources are conducting the integration testing for the module, such as testing environments, collecting test data, and leveraging appropriate test tools.

A.11.9.2.8. The Contractor shall provide testing support to the other DE Component Contractor(s), if any, for all phases of testing as defined in the SILC.

A.11.9.2.9. The Contractor shall participate in and support User Acceptance Testing (UAT) for configuration items during DDI and O&M, which includes creating UAT test cases, providing subject matter expert resources throughout UAT execution, and assisting with planning. All UAT activities shall be done in conjunction with MMPVP and applicable DE Component Contractor(s), if any, and subject to TennCare oversight and approval.

A.11.9.2.10. The Contractor shall mask any Sensitive Data from the production environment for use in non-production environments unless the data owner authorizes the use of Sensitive Data in the non-production environment.

A.11.9.2.11. The Contractor shall complete the activities and Deliverables assigned to "Module Solution Vendor" in the Test Management Standard RACI table based on the identified role (noted as "A", "C", "I", or "R").

A.11.9.2.12. The Contractor shall complete and/or update Deliverables assigned to the "Module Solution Vendor" in the Test Management Standard RACI table based on the identified role (noted as "A", "C", "I", or "R").

A.11.10. IT Service Management

A.11.10.1. Standard Operating Procedure Manual

A.11.10.1.1. The Contractor shall refer to the TennCare IT Service Management (ITSM) Standard and TennCare IT Service Management RACI in Attachment C, Procurement Library, to develop all the ITSM processes, activities, and tasks required for ITSM in this Section A.11.10 and Contract and document the required ITSM procedures in the Standard Operating Procedures (SOP) Manual for TennCare approval.

A.11.10.1.2. The Contractor shall follow and execute all procedures and processes required for the DE Component in the approved SOP Manual.

A.11.10.1.3. The Contractor shall build and maintain a delimited SOP Manual for the DE Component for the purposes of easily onboarding new resources and consistent operation of the DE Component. The SOP Manual shall also be made available to MMPVPs. TennCare may require a SOP Manual to be written for specific system support functions. The Contractor shall provide any and all tools necessary to fulfil the SOP Manual obligations related to executing these capabilities.

A.11.10.1.4. The Contractor shall incorporate the outcomes and recommendations of the Continuous Improvement Process (CIP) into SOP Manual updates.

A.11.10.1.5. The Contractor shall maintain the SOP as the document of record for DE Component activities, maintain the SOP under Configuration Management control, and update SOP documentation as a standard part of the change management process.

A.11.10.2. Module Support Team

A.11.10.2.1. The Contractor shall provide twenty-four (24) hours per day x seven (7) days per week x three hundred sixty-five (365) days per year production support to coordinate service issue identification, investigation, and diagnosis in cooperation with TennCare, the IS Contractor, and MMPVPs. The DE Component Contractor shall not be responsible for the direct activities of ISL or other Module Contractors' Service Desks.

A.11.10.2.2. The Contractor shall provide a staffed Module Support Team during normal business hours. Normal business hours are defined as 7:00 AM to 7:00 PM Central, Monday through Friday, excluding State observed holidays.

A.11.10.2.3. The Contractor shall provide an On-Site, in-person Module Support Team for DE Component functions at TennCare facilities on an as-requested, temporary basis.

A.11.10.2.4. The Contractor shall have staff on-call and available outside of normal business hours as required to maintain compliance with the TennCare SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.11.10.2.5. The Contractor shall utilize the TennCare-approved ITSM tool to provide Module Support services for the DE Component and record and manage service-related activities.

A.11.10.2.6. The Contractor shall manage and track all DE Component-related ITSM incidents to resolution and provide recurring status updates in coordination with the IS Contractor ITSM reporting procedures or upon request from TennCare.

A.11.10.2.7. The Contractor shall adhere to TennCare-approved multi-tiered support structure and escalation procedures that include security Incident Management and critical Problem (e.g., system outage) processes. The support structure shall include a Module Support Team appropriately aligned with the TennCare ITSM Standard for the Service Desk Function.

i. The IS Contractor shall provide front line Service Desk support that accounts for Tier I Service Desk support consisting of services to address general issues and routing of higher complexity issues requiring Tier II Level Support to the appropriate IS Component and/or Module Support Team.

A.11.10.2.8. The Contractor shall provide Tier II Level Support, consisting of support services that require technical resources who have specialized skills related to the DE Component.

A.11.10.2.9. The Contractor shall provide Tier III Level Support requiring technical expertise related to the DE Component.

A.11.10.2.10. The Contractor shall be responsible for consolidation tracking of Tier II and Tier III incidents to resolution in coordination with the IS Contractor, reporting to TennCare, and informing MMPVPs of configuration item(s) changes that impact TennCare activities.

A.11.10.2.11. The Contractor shall be responsible for reporting the resolution results to the Tier I Service Desk.

A.11.10.2.12. The Contractor shall develop an incident priority matrix for Module Support Team Incident Management activities subject to TennCare approval.

A.11.10.2.13. The Contractor shall implement bi-directional integrations and associated transformation mapping between the Contractor's Incident Management system and TennCare's ITSM system in collaboration with TennCare, the IS Contractor, and MMPVPs.

A.11.10.2.14. The Contractor shall integrate Contractor's Governance, Risk, and Compliance (GRC) tools with the TennCare approved ITSM tool to support tracking and resolution of all GRC related vulnerabilities. The Contractor may use TennCare GRC tools identified in the TennCare Preferred Technology Standard or Contractor's own GRC tools for this purpose with TennCare approval.

A.11.10.2.15. The Contractor shall provide reoccurring status updates on GRC activities in coordination with the IS Contractor on a timeline defined by TennCare.

A.11.10.2.16. The Contractor shall monitor the production environment twenty-four (24) hours per day x seven (7) days per week x three hundred sixty-five (365) days per year and develop, maintain, and manage a plan to monitor every operation that affects the DE Component and associated configuration items (e.g. network, software, interfaces, services, data manipulation).

A.11.10.2.17. The Contractor shall comply with the requirements of the ITSM Standard for additional service management functions, processes, and activities.

A.11.10.3. IT Operations Management

A.11.10.3.1. The Contractor shall establish a centralized operations management center that acts as the central coordination point for managing various classes of events, detecting incidents, managing routine operational activities, and reporting on the status or performance of DE Component technology components.

A.11.10.3.2. The Contractor's IT Operations Management shall have the capability to intake requests from the IS Contractors Tier 1 Service Desk via the TennCare ITSM tool from internal and external stakeholders interacting with the DE Component.

A.11.10.3.3. The Contractor shall integrate the DE Component with the ISL and adhere to the operational procedures as defined by TennCare.

A.11.10.3.4. The Contractor shall be responsible for planning and managing the execution of software tasks according to schedule for the DE Component in coordination with the IS Contractor and MMPVP activities.

A.11.10.3.5. The Contractor shall be responsible for compliance with TennCare standards during IT operations and support the EDW Contractor's, if applicable, and IS Contractor's enforcement activities for DE ITSM processes.

A.11.10.3.6. The Contractor shall automate job scheduling using software tools that run batch or online tasks at specific times, where applicable.

A.11.10.3.7. The Contractor shall be responsible for monitoring and control of IT services for the DE Component.

A.11.10.3.8. The Contractor shall maintain compliance with the SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.11.10.4. Technical Management

A.11.10.4.1. The Contractor shall be responsible for the technical management function of the DE Component, providing technical skills and capabilities in support of TennCare services, and management of the DE Component. The Contractor shall define the roles of support teams, tools, processes, and procedures required to achieve acceptable service levels as defined by TennCare.

A.11.10.4.2. The Contractor shall be responsible for management of the DE Component to include, at a minimum, the following activities:

i. Operating system support;

ii. License management;

iii. Third-level support;

iv. Application management;

v. Procurement advice;

vi. System security;

vii. Definition and management of virtual servers;

viii. Assistance to capacity management;

ix. Ongoing maintenance; and

x. Decommissioning and disposal of old servers.

A.11.10.4.3. The Contractor shall be responsible for Database administration to ensure the optimal performance, security, and functionality of Databases managed.

A.11.10.4.4. The Contractor shall be responsible for network management activities to ensure proper functioning of TennCare network performance and collaborating with third-party network suppliers.

A.11.10.4.5. The Contractor shall be responsible for internet/web management process to cover both intranet and internet.

A.11.10.4.6. The Contractor shall be responsible for integration into TennCare directory services activities to ensure process information about IT infrastructure is available online with appropriate user access rights as defined by TennCare.

A.11.10.4.7. The Contractor shall be responsible for the desktop support process and the overall responsibility for all of the Contractor's desktop and laptop computer hardware, software, and peripherals.

A.11.10.4.8. The Contractor shall install the TennCare's JVPN client onto Contractor-owned laptop/desktop machines in order to access tools and instruments on the State's network. TennCare will not provide TennCare-owned laptops to the Contractor.

A.11.10.5. Application Management

A.11.10.5.1. The Contractor shall be responsible for managing DE Component-related applications throughout the application lifecycle to include design, build, testing (including user and accessibility testing), deploy, configure, operate, optimize, and transition activities as related to service management.

A.11.10.5.2. The Contractor shall support the planning of the service agreements/contracts and IT infrastructure in coordination with TennCare and MMPVPs to ensure alignment with TennCare's enterprise architecture and required levels of availability needed by TennCare.

A.11.10.5.3. The Contractor shall organize the DE Component application management teams according to categories of applications or Modules they support.

A.11.10.5.4. The Contractor shall be responsible for continually measuring the DE Component application performance against the service levels.

A.11.10.6. Continuous Improvement Process (CIP)

A.11.10.6.1. The Contractor shall be responsible for managing a Continuous Improvement Process (CIP) to include repeatable, defined, and efficient management processes for optimization of all DE Component-related Services throughout the entire Service Lifecycle.

A.11.10.6.2. The Contractor shall manage the CIP with TennCare-designated Key Personnel resources.

A.11.10.6.3. The Contractor's engagement leadership shall review quarterly, at a minimum, the effectiveness of the entire CIP approach to ensure appropriate identification, management, and implementation of service improvements in alignment with TennCare's objectives and approach for the CIP.

A.11.10.6.4. The Contractor shall be responsible for developing and implementing a CIP that aligns with Industry Standards and Policies (e.g., ITIL or Six Sigma) and is approved by TennCare.

A.11.10.6.5. The Contractor shall continuously identify and present improvement opportunities within each service function, process, and activity to maximize the service performance, value, and functionality to TennCare for feasibility reviews at a cadence determined by TennCare.

A.11.10.6.6. The Contractor shall manage a CIP backlog of improvement opportunities identified jointly by TennCare and the Contractor for all activities to maximize performance, value, and functionality.

A.11.10.6.7. The Contractor shall track in the CIP backlog all relevant data related to individual improvement opportunities from identification to post-implementation analysis information.

A.11.10.6.8. The Contractor shall present implementation options and supporting materials, including relevant documentation, demonstrations, results of quantitative analysis, or other information as requested by TennCare, for CIP backlog items or specific items requested by TennCare for review and potential approval.

A.11.10.6.9. The Contractor shall implement TennCare approved service improvements as an output of the CIP through TennCare's change management process.

A.11.10.6.10. The Contractor shall develop reports and Dashboards, as specified by TennCare, to support the CIP and make them available for TennCare review. Reports and Dashboards, including the underlying KPIs, shall be reviewed by TennCare on

a cadence approved by TennCare and modified by the Contractor in order to mature the CIP and produce the best results.

A.11.10.6.11. The Contractor shall incorporate defined processes to conduct service reviews of ITSM activities for CIP opportunities.

A.11.10.6.12. The Contractor shall identify opportunities related to DE Component to improve the services across the enterprise and enhance service offerings to Tennessee citizens.

A.11.10.6.13. The Contractor shall incorporate into service management processes regularly performed process assessments, benchmarking, and auditing activities, at a minimum monthly for each ITSM process or a timeline defined by TennCare, to drive innovation and improvement.

A.11.10.6.14. The Contractor shall be responsible for suggesting initiatives to improve services and quality for TennCare operations relating to the DE Component at a cadence agreed upon by TennCare.

A.11.10.6.15. The Contractor shall be responsible for tracking the progress of CIP initiatives through post-implementation to confirm expected benefits have been realized and document lessons learned.

A.11.10.6.16. The Contractor shall provide feedback to the CIP service review and evaluation processes for future planning initiatives.

A.11.10.7. Service Strategy

A.11.10.7.1. The Contractor shall support the ongoing refinement of the TennCare Service Strategy through collaborative activities with the IS Contractor and MMPVPs in alignment with TennCare priorities and goals.

A.11.10.7.2. The Contractor shall monitor patterns of DE Component business activity and provide suggestions for performance optimization for TennCare approval.

A.11.10.7.3. The Contractor shall perform activities to confirm production services perform as expected from a business user perspective.

A.11.10.7.4. The Contractor shall support TennCare in identification and resolution of known performance issues related to IT services affecting business processes.

A.11.10.7.5. The Contractor shall support TennCare's Service Strategy financial management activities related to IT services.

A.11.10.7.6. The Contractor shall support TennCare's Service Strategy strategic management activities related to IT services.

A.11.10.8. Service Design

A.11.10.8.1. Design Coordination

A.11.10.8.1.1. The Contractor shall comply with all applicable TennCare Policies and Standards including, but not limited to TennCare Policies and Standards located in Attachment C, Procurement Library, and be responsible for defining methods consisting of, at a minimum, design acceptance criteria, policies, principles, procedures, and documentation, related to service design practices for MMPVP components and users.

A.11.10.8.1.2. The Contractor shall coordinate with the IS Contractor on DE Component design activities across projects and

changes, managing schedules, resources and conflicts, and suppliers and support teams, where required.

A.11.10.8.1.3. The Contractor shall be responsible for the scheduling of both the service provider and customer consumer resources to ensure involvement of resources to create an accurate and complete design.

A.11.10.8.1.4. The Contractor shall use formal risk assessment and management techniques to manage risks associated with design activities and reduce the number of issues traced to poor design and/or non-compliant architecture.

A.11.10.8.1.5. The Contractor shall be responsible for continually improving TennCare service design practice, to ensure:

i. Adherence to defined policies and methods;

ii. No conflicts with other ongoing design efforts;

iii. Design milestones are being met; and

iv. Timely development of comprehensive designs that will support the achievement of the required TennCare outcomes.

A.11.10.8.1.5. The Contractor shall contribute to IS Contractor and MMPVP Service Design activities as approved by TennCare.

A.11.10.8.2. Service Portfolio and Catalog Management

A.11.10.8.2.1. The Contractor shall coordinate with TennCare and the IS Contractor for documenting service definitions and descriptions into a comprehensive TennCare Service Catalog and integration of the TennCare Service Catalog with the appropriate Configuration Management tools in accordance with the ITSM Standard.

A.11.10.8.2.2. The Contractor shall define a process for the production and maintenance of the Service Catalog content for TennCare approval.

A.11.10.8.2.3. The Contractor shall contribute to the maintenance of the approved TennCare Service Catalogs and Portfolio.

A.11.10.8.2.4. The Contractor shall manage the DE Component Service Catalog under formal change management control.

A.11.10.8.2.5. The Contractor shall provide TennCare the necessary inputs for MMP-related services into TennCare's Service Portfolio and Service Catalog.

A.11.10.8.2.6. The Contractor shall provide the relevant input to TennCare, the IS Contractor, and MMPVPs on an as-needed basis.

A.11.10.8.2.7. The Contractor shall utilize the TennCare-approved Service Portfolio and Service Catalog system to support issue resolution.

A.11.10.8.2.8. The Contractor shall have an in-depth knowledge and understanding of all TennCare SLAs, collaborate on refinements and standardization of SLAs for systems integrated into the DE Component, and support

TennCare in the drafting of future SLA documentation in coordination with TennCare-identified vendor partners.

A.11.10.8.2.9. The Contractor shall conduct review meetings with TennCare and MMPVPs and produce standard reports to review the service achievement for TennCare and MMPVPs in the previous time periods and anticipated issues for the future time periods as defined by TennCare.

A.11.10.8.2.10. The Contractor shall perform active monitoring of the DE Component service performance and develop an automated process to alert the IS Contractor and TennCare of service degradation or anomalies.

A.11.10.8.2.11. The Contractor shall be responsible and accountable for ongoing monitoring and reporting on performance against any service levels requested by and agreed upon with TennCare. At a frequency established by TennCare, the Contractor shall perform service level reviews. Following the Contractor's service level review, the Contractor may recommend modifications to TennCare. Service Level Agreements may be modified by mutual agreement between the Contractor and TennCare.

A.11.10.8.2.12. The Contractor shall develop a TennCare approved operational reporting document consistent with the TennCare SILC and defined in the TennCare SILC RACI and Deliverables to support transparent and consistent end-to-end management of IT services leveraging a consistent set of processes, activities, and tools. The tracking and reporting on key performance metrics shall drive continuous improvement processes and compliance with standards and service levels.

A.11.10.8.3. Capacity Management

A.11.10.8.3.1. The Contractor shall be responsible for monitoring capacity data for the DE Component.

A.11.10.8.3.2. The Contractor shall be responsible for defining capacity planning procedures and associated documentation for a standardized approach for the DE Component capacity management for TennCare approval.

A.11.10.8.3.3. The Contractor shall be responsible for analysis, investigation, and notification to TennCare of IT service capacity issues for the DE Component.

A.11.10.8.3.4. The Contractor shall be responsible for reviewing capacity statistics for optimization and improvement opportunities and report this information in the CIP process.

A.11.10.8.3.5. The Contractor shall be responsible and accountable for all activities required for identifying and managing appropriate system capacity for the DE Component-related system, which include production and non-production environments (e.g., development, test, training, etc.). This includes requirements identification, planning, management, reporting, and augmentation of system capacity and performance.

A.11.10.8.3.6. The Contractor shall be responsible for identifying performance and capacity drivers, understanding the impact to the program, and developing solutions to accommodate potential capacity and performance demands. The DE Component shall be designed to easily scale for additional capacity to meet emergency demands.

A.11.10.8.3.7. The Contractor shall follow the agreed upon schedule for developing models, utilizing tools, and developing solutions that avoid any disruption or degradation of service.

A.11.10.8.3.8. The Contractor shall ensure the requirements of this subsection include development of a complete set of metrics (in alignment with the program's CIP) to measure and manage system drivers including business drivers (e.g., population, number of applicants, and regulatory changes), the infrastructure (e.g., central processing unit, memory, bandwidth, transfer rates, and storage), and other system/code-related challenges (e.g., SQL code, Database configurations, and optimal system tuning opportunities).

A.11.10.8.3.9. The Contractor shall work with TennCare, IS Contractor, and MMPVPs to ensure the appropriate system capacity and performance is delivered.

A.11.10.8.4. Availability Management

A.11.10.8.4.1. The Contractor shall be responsible for defining availability planning procedures and associated documentation including measures, targets, underpinning service agreements/contracts, and criteria, for a standardized approach for DE Component availability management for TennCare approval.

A.11.10.8.4.2. The Contractor shall be responsible for monitoring availability data for the DE Component.

A.11.10.8.4.3. The Contractor shall be responsible for analysis, investigation, and notification to TennCare of IT service availability issues for the DE Component.

A.11.10.8.4.4. The Contractor shall use simulation, modeling, and load test tools in order to ensure that the DE Component can operate under stress conditions.

A.11.10.8.4.5. The Contractor shall be responsible for defining, analyzing, planning, measuring, and improving all aspects of the availability related to the DE Component production and test environments.

A.11.10.8.5. IT Service Continuity Management

A.11.10.8.5.1. The Contractor shall develop requirements and continuity plans for managing risks that could impact Services to ensure that the DE Component can always provide minimum agreed SLAs.

A.11.10.8.5.2. The Contractor shall ensure development, use, and updating of continuity plans at intervals determined by TennCare for DE Component Services.

A.11.10.8.5.3. The Contractor shall ensure testing of components critical to recovery plans at a cadence by TennCare.

A.11.10.8.6. Information Security Management

A.11.10.8.6.1. The Contractor represents and warrants they have a complete understanding of TennCare security requirements and standards.

A.11.10.8.6.2. The Contractor shall support production, updating, and improvement in the development of security policies and controls.

A.11.10.8.6.3. The Contractor shall fully support TennCare in implementing approved security policies.

A.11.10.8.6.4. The Contractor shall be responsible for conducting assessments of information assets and risks, at a cadence approved by TennCare, and providing reporting to TennCare.

A.11.10.8.7. Performance Management

A.11.10.8.7.1. The Contractor shall monitor and analyze performance data to identify DE Component performance issues and improvement opportunities.

A.11.10.8.7.2. The Contractor shall analyze the performance data of the DE Component operating on the DE for patterns, trends, and insights to enhance the performance of TennCare enterprise solutions.

A.11.10.8.7.3. The Contractor shall be responsible for investigating performance issues related to DE Component and associated solution components to resolution and providing relevant documentation to TennCare.

A.11.10.8.7.4. The Contractor shall support TennCare, IS Contractor, and MMPVPs in the design and implementation of high-performance DE Component solutions to achieve and exceed minimum acceptable service levels.

A.11.10.8.7.5. The Contractor shall be responsible for reviews of the service delivery framework, at a cadence approved by TennCare, for performance improvements to:

i. Ensure that service design activities incorporate performance improvement opportunities and outputs from the CIP process;

ii. Ensure that performance improvement opportunities drive service strategy development; and

iii. Ensure the performance improvements are incorporated into the Service Lifecycles and governance structures expediently.

A.11.10.9. Service Transition

A.11.10.9.1. Change Management

A.11.10.9.1.1. The Contractor's change management process shall include clearly defined procedures for documentation, assessment, and categorization of any change related to ITSM affecting the DE Component and integrations.

A.11.10.9.1.2. The Contractor shall adhere to TennCare policies regarding Change Management in coordination with the IS Contractor.

A.11.10.9.1.3. The Contractor's change management process shall include clearly defined procedures for risk and impact analysis across the DE.

A.11.10.9.1.4. The Contractor shall coordinate change, build, and test activities for the DE Component.

A.11.10.9.1.5. The Contractor's change management process shall include procedures to authorize change deployment for the DE Component in alignment with continuous development/integration best practices as approved by TennCare.

A.11.10.9.1.6. The Contractor's change management process shall include procedures for review and closure of change records that promotes transparency and visibility to the DE Component.

A.11.10.9.1.7. The Contractor shall log all system changes within TennCare's ITSM tool for TennCare to evaluate and approve.

A.11.10.9.2. Change Evaluation

A.11.10.9.2.1. The Contractor's change management process shall include an evaluation process to ensure that a change is evaluated from different perspectives due to TennCare's multi-cloud/tier environment.

A.11.10.9.2.2. The Contractor shall adhere to TennCare policies regarding Change Evaluation in coordination with the IS Contractor.

A.11.10.9.2.3. The Contractor's change management process shall include detailed risk and evaluation procedures for proposed changes to transparently identify the predicted/expected results of the proposed change of the TennCare architecture.

A.11.10.9.2.4. The Contractor's change management process shall include detailed risk and evaluation procedures for implemented changes to transparently determine:

i. Benefit realized from change;

ii. Actual benefit realized vs predicted;

iii. Lessons learned from change; and

iv. Potential CIP opportunities.

A.11.10.9.3. Transition Planning and Support

A.11.10.9.3.1. The Contractor shall be responsible for defining the roles, policies, and methods related to administration of Service Transition and planning for the DE Component and ISL components and users to include at a minimum:

i. Managing of integrated planning activities for Service Transitions;

ii. Managing of Service Transition changes;

iii. Managing issues and risks;

iv. Managing support for tools and Service Transition processes;

v. Communication to stakeholders;

vi. Monitoring of Service Transition performance; and

vii. Template for individual Service Transition Plan(s).

A.11.10.9.3.2. The Contractor shall adhere to TennCare policies regarding Asset and Configuration Management in coordination with the IS Contractor.

A.11.10.9.3.3. The Contractor shall be responsible for development and continued refinement of Service Transition models for use in the DE Component.

A.11.10.9.3.4. The Contractor shall be responsible for defining the overall approach to organizing Service Transitions and allocating resources in the DE Component for TennCare approval.

A.11.10.9.3.5. The Contractor shall be responsible for coordination of all DE Component Service Transition activities across projects, changes, managing schedules, resources, conflicts, and suppliers and support teams, where required.

A.11.10.9.3.6. The Contractor shall be responsible for the scheduling of both the service provider and customer resources to ensure involvement of the appropriate resources to create an accurate and complete design.

A.11.10.9.3.7. The Contractor shall be responsible for monitoring and reporting progress on Service Transitions for DE Component services to include at a minimum:

i. Transition status updates;

ii. Configuration compliance reviews; and

iii. Evaluation reports.

A.11.10.9.3.8. The Contractor shall contribute to IS Contractor Service Transition activities as approved by TennCare.

A.11.10.9.4. Release and Deployment Management

A.11.10.9.4.1. The Contractor shall be responsible for release preparation activities to include assessing DE Component potential deployments and developing concrete deployment plans in coordination with the IS Contractor and MMPVPs.

A.11.10.9.4.2. The Contractor shall adhere to TennCare policies regarding Release and Deployment Management in accordance with the IS Contractor.

A.11.10.9.4.3. The Contractor's Release and Deployment Management process shall include procedures for the development of release and build documentation, acquisition and testing of input configuration items and components, release packaging content, and procedures for the building and management of the test environments. The Contractor shall ensure that these procedures required by this subsection are included in the SOP.

A.11.10.9.4.4. The Contractor's Release and Deployment Management process shall include procedures for release deployment

activities to include review of deployment process and verification service functionality is as implemented.

A.11.10.9.4.5. The Contractor's Release and Deployment Management process shall include procedures for supporting new or changed Services based on category to determine appropriate early life support needs for each deployment.

A.11.10.9.4.6. The Contractor's Release and Deployment Management process shall include procedures for release review and closure activities that at a minimum addressed:

i. Deployed processes;

ii. Transfer/deployed service;

iii. Decommissioning and service retirement;

iv. Removal redundant assets; and

v. Assessments of completed deployment.

A.11.10.9.4.6. The Contractor shall develop formal Release and Deployment Management processes and procedures to effectively govern the Release and Deployment Management process while coordinating releases with the IS Contractor and impacted MMPVPs and incorporating industry-standard continuous integration and deployment approaches for cloud environments to ensure all parties are ready for releases.

A.11.10.9.4.7. The Contractor shall provide technical release notes in advance of each release.

A.11.10.9.4.8. The Contractor shall ensure that all code releases follow best practices for separation of duties (e.g. developers should never deploy code, etc.).

A.11.10.9.4.9. The Contractor shall perform all deployments other than emergency releases during non-business hours.

A.11.10.9.4.10. The Contractor shall coordinate all releases with the IS Contractor and relevant MMPVPs to avoid any potential adverse impacts on MMIS Modules from deployments.

A.11.10.9.5. Service Validation and Testing

A.11.10.9.5.1. The Contractor shall be responsible for planning and designing test activities for the DE Component in coordination with the IS Contractor and MMPVPs.

A.11.10.9.5.2. The Contractor shall adhere to TennCare policies regarding Service Validation and Test Management in coordination with the IS Contractor.

A.11.10.9.5.3. The Contractor shall be responsible for verifying test plans and designs for the DE Component in coordination with the IS Contractor and MMPVPs.

A.11.10.9.5.4. The Contractor shall be responsible for preparing test environments for the DE Component in coordination with the IS Contractor and MMPVPs.

A.11.10.9.5.5. The Contractor shall be responsible for development of supplemental test cases for testing activities for the DE

Component in coordination with the IS Contractor and MMPVPs.

A.11.10.9.5.6. The Contractor shall be responsible for evaluating testing exit criteria for the DE Component in coordination with the IS Contractor and MMPVPs.

A.11.10.9.6. Service Asset and Configuration Management

A.11.10.9.6.1. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of Service Asset and Configuration Management activities.

A.11.10.9.6.2. The Contractor shall adhere to TennCare policies regarding Service Asset and Configuration Management in coordination with the IS Contractor.

A.11.10.9.6.3. The Contractor shall be responsible for ensuring that the process for adding, modifying, or removing a CI is properly managed for the DE Component.

A.11.10.9.6.4. The Contractor shall be responsible for actively accounting for CI status and reporting activities as defined by TennCare.

A.11.10.9.6.5. The Contractor shall be responsible for verification and accounting of CI status to include audits and assessments, at a cadence approved by TennCare, to encourage proper Configuration Management throughout TennCare.

A.11.10.9.7. Knowledge Management

A.11.10.9.7.1. The Contractor shall be responsible for defining a DE Component Knowledge Management strategy for TennCare approval and alignment of the DE Component knowledge management processes to the TennCare Enterprise Knowledge Management Strategy.

A.11.10.9.7.2. The Contractor shall adhere to TennCare policies regarding Knowledge Management in coordination with the IS Contractor.

A.11.10.9.7.3. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of Knowledge Management activities.

A.11.10.9.7.4. The Contractor shall be responsible for coordinating DE knowledge sharing activities across the enterprise in conjunction with TennCare and the IS Contractor.

A.11.10.9.7.5. The Contractor shall be responsible for establishment of DE Component data and information requirements and associated information architecture definitions.

A.11.10.9.7.6. The Contractor shall be responsible for establishing DE Component data and information management procedures and providing evaluation reviews to identify improvement opportunities, at a cadence approved by TennCare.

A.11.10.9.7.7. The Contractor shall be responsible for identification, collection, analyzing, storing, and sharing of knowledge and information across the MMPVP landscape for the purpose of improving efficiency by reducing the need and effort to discover knowledge.

A.11.10.9.7.8. The Contractor shall be responsible for drafting documentation and content related to knowledge management, conducting a formal technical and editorial review, and publishing the information in an easily accessible online location.

A.11.10.9.7.9. The Contractor shall provide online help for all features, functions, and data element fields as well as descriptions and resolutions for error messages using help features (e.g. indexing, searching, tool tips, and context-sensitive help topics).

A.11.10.10. Service Operations

A.11.10.10.1. Event Management

A.11.10.10.1.1. The Contractor shall be responsible for the management of DE Component event notifications.

A.11.10.10.1.2. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of Event Management activities.

A.11.10.10.1.3. The Contractor shall be responsible for management of DE Component event detection.

A.11.10.10.1.4. The Contractor shall be responsible for correlating and filtering events and routing or receiving event related information, as appropriate.

A.11.10.10.1.5. The Contractor shall be responsible for ensuring that all components of the DE Component are designed to support Event Management, i.e. provide meaningful error messages.

A.11.10.10.1.6. The Contractor shall be responsible for categorization of events in alignment with the TennCare Integration Standard.

A.11.10.10.1.7. The Contractor shall be responsible for reviewing the events that have been resolved appropriately as defined by TennCare.

A.11.10.10.1.8. The Contractor shall automate all event management monitoring and notification processes, unless otherwise approved by TennCare.

A.11.10.10.2. Incident Management

A.11.10.10.2.1. The Contractor shall be responsible for management of DE Component incident registration and categorization activities.

A.11.10.10.2.2. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of Incident Management activities for the respective DE Component.

A.11.10.10.2.3. The Contractor shall be responsible for management of DE Component incident prioritization activities.

A.11.10.10.2.4. The Contractor shall be responsible for management of DE Component incident investigation and diagnosis.

A.11.10.10.2.5. The Contractor shall be responsible for management of DE Component incident resolution and closure.

A.11.10.10.2.6. The Contractor shall be responsible for providing a consolidated view of the DE Component to include event and Incident Management along with other appropriate

processes that shall enable TennCare and the IS Contractor to have full visibility of the DE Component.

A.11.10.10.3. Request Fulfillment Management

A.11.10.10.3.1. The Contractor shall be responsible for request registration for DE Component services.

A.11.10.10.3.2. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support for Request Fulfillment activities, in a manner consistent with TennCare Policies.

A.11.10.10.3.3. The Contractor shall adhere to TennCare policy for DE Component Request Fulfillment activities.

A.11.10.10.3.4. The Contractor shall be responsible for validating DE Component service requests.

A.11.10.10.3.5. The Contractor shall be responsible for categorization and prioritization of service requests.

A.11.10.10.3.6. The Contractor shall be responsible for review and resolution service requests.

A.11.10.10.3.7. The Contractor shall be responsible for closure of DE Component service requests.

A.11.10.10.4. Access Management

A.11.10.10.4.1. The Contractor shall be responsible for DE Component access management requisition via the IAM in coordination with TennCare.

A.11.10.10.4.2. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of access management activities.

A.11.10.10.4.3. The Contractor shall be responsible for management of the DE Component access verification and validation of requisition activities.

A.11.10.10.4.4. The Contractor shall be responsible for management of the DE Component incident registration and categorization.

A.11.10.10.4.5. The Contractor shall be responsible for monitoring, tracking, and controlling the access to the DE Component.

A.11.10.10.4.6. The Contractor shall be responsible for de-provisioning access for users and the DE Component.

A.11.10.10.5. Problem Management

A.11.10.10.5.1. The Contractor shall be responsible for DE Component Problem Management.

A.11.10.10.5.2. The Contractor shall support TennCare and IS Contractor with the coordination, detection, and logging of Problem Management activities.

A.11.10.10.5.3. The Contractor shall be responsible for the development of Problem Management procedures and documentation to proactively address Problems in service operations or as part of CIP for use for the DE Component. These procedures shall include precise steps for investigation, diagnosis, resolution,

and closure of Problems. These procedures shall be included in the SOP.

A.11.11. Turnover

A.11.11.1. If applicable, the Contractor shall cooperate with TennCare in transitioning the DE Component and responsibilities of this Contract to TennCare, authorized contractor, and/or successor contractor upon termination or expiration of this Contract.

A.11.11.2. The Contractor shall deliver to TennCare, or its authorized representative, all Contract-related records and data in a format specified by TennCare, thirty (30) calendar days prior to Contract expiration or thirty (30) calendar days after TennCare's request.

A.11.11.3. The Contractor shall ensure that a Turnover Plan is delivered and approved by TennCare as part of the Operational Readiness Review. The Contractor shall also provide an updated version of the Turnover Plan at a minimum of one hundred eighty (180) calendar days prior to the Contract end date. The Turnover Plan shall include:

A.11.11.3.1. A timeline with milestones for the Turnover to include planning, execution, and implementation approval;

A.11.11.3.2. Description of maintenance process for Turnover documentation and Artifacts throughout the life of the Contract; and

A.11.11.3.3. Any additional information requested by TennCare in a Control Memorandum.

A.11.11.4. If applicable, the Contractor shall carry out an orderly, cooperative, comprehensive, and controlled transition to TennCare and/or the successor Contractor, and shall provide the below described Turnover Deliverables, services, and support:

A.11.11.4.1. Security profiles of the platform users and service accounts in a Microsoft Word document or Microsoft Excel spreadsheet format; and

A.11.11.4.2. Turnover Deliverables that are considered TennCare customizations, data, and assets that are non-proprietary aspects of the COTS solution as requested by TennCare and in a format acceptable to TennCare.

A.11.11.5. The Contractor shall provide post-Turnover support for up to one hundred twenty (120) calendar days, including Deliverables and associated activities specified in a Control Memorandum and agreed to by TennCare.

A.11.11.6. The Contractor shall complete financial reconciliation of this Contract, including liquidated or financial consequences, if applicable.

A.11.11.7. The Contractor's obligations under this section shall be at no additional cost to TennCare and shall survive the termination of this Contract.

A.12. Administrative Requirements

A.12.1. CMS Certification

A.12.1.1. In order to maximize the Enhanced Federal Financial Participation (EFFP) match for the DE, TennCare requires the DE Solution to be certified by CMS holistically back to Day 1 of the Operations Phase for the first DE Component to achieve Go-Live and to obtain certification within twelve (12) months of the DSS Go-Live date or as mutually agreed upon with TennCare and CMS. The Contractor(s) shall provide specific Artifacts and documentation to TennCare, in accordance with the criteria established by CMS for certification and the timelines delineated by CMS and TennCare, as evidence that the DE meets CMS' certification requirements through every SILC phase. The Contractor shall work at the

direction of TennCare's certification team throughout the certification process. The Contractor shall collaborate with TennCare in providing all certification related Deliverables as defined in the TennCare Solution Implementation Lifecycle. If CMS changes any part of the certification process, the Contractor shall, at no additional cost to TennCare, provide all documentation and undertake all activities required by the new CMS Certification process.

A.12.1.2. The Contractor shall collaborate with TennCare to provide a Certification Plan that describes the process the Contractor will use to plan, manage, and execute any CMS Certification of the solution. The Contractor shall remain current with changes made to the certification requirements and update its plan accordingly throughout the certification lifecycle. The plan will include, but is not limited to, all Federal certification requirements and Gate Review requirements specified under the current certification process.

A.12.1.3. The Contractor shall develop a Certification Crosswalk that describes how the Contractor(s)'s evidence Artifacts, Deliverables, and other control documentation align with Federal certification requirements, evaluation criteria, milestone reviews, and reporting.

A.12.1.4. The Contractor shall support CMS Certification for all components included in the scope of the Data Ecosystem. The Contractor shall support certification milestone reviews during the implementation and O&M phases by addressing certification requirements including, but not limited to, creating all relevant certification-related Artifacts as defined in the TennCare Solution Implementation Lifecycle and CMS Certification requirements.

A.12.1.5. Prior to Go-Live of the DE Component, the Contractor shall engage an outside party to conduct a Third-Party Security and Privacy Assessment, per CMS' guidelines and TennCare's direction. This third-party assessment must be completed prior to Go-Live and all reports and findings from this assessment available for review by TennCare, CMS, and MMPVPs. Additional reports required by CMS will be provided at no additional cost to TennCare. The Contractor will also be required to monitor findings, continue to assess the system for security and privacy vulnerabilities, and draft, share, manage, and report on a POA&M for these findings.

A.12.1.6. The Contractor shall integrate the certification timeline and tasks into the Contractor's Project Schedule as defined in the TennCare SILC RACI and Deliverables. The Contractor(s) shall provide in the Project Schedule all certification related tasks and timelines. Prior to the Go-Live date, as defined in Project Schedule, the DE will be evaluated for certification by CMS using the agreed upon version of the Certification Requirements. The Contractor shall provide to TennCare for review, no later than the date defined in the Project Schedule, all finalized DE Component Artifacts and documentation that CMS requires. Following the Go-Live date as defined in Project Schedule, the DE will be evaluated for certification by CMS using the agreed upon version of the Certification Requirements. CMS requires the DE Solution to be in production for six (6) months prior to submission of TennCare's initial certification request, which is anticipated to be submitted to CMS on the date defined in Project Schedule. Any remediation recommended by CMS throughout this certification process will be undertaken by the Contractor at no additional cost to TennCare and will be done in accordance with the SLAs in Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.12.1.7. At no additional cost to TennCare, the Contractor shall participate and provide support as needed to the MMIS Module Vendors for module certification activities including participating in planning activities, meetings, and other activities as required by CMS.

A.12.1.8. The Contractor shall provide a Certification Manager to collaborate and coordinate with TennCare and the MMPVPs in order to support TennCare in and

throughout the entire CMS/Federal certification process. The Contractor shall provide both system and business operations staff to support TennCare in the completion of all CMS-required certification items. The Contractor will provide subject matter expertise to answer questions or provide insight during the certification process, including On-Site, in-person interviews.

A.12.2. Training

A.12.2.1. The Contractor shall collaborate with TennCare and MMPVPs for on-going training, technical knowledge transfer, and assessment of program effectiveness.

A.12.2.2. The Contractor shall collaborate with TennCare and MMPVPs to follow and execute industry leading practices, standards, and trends for delivery and focus of training.

A.12.2.3. The Contractor shall ensure that Contractor has sufficient, appropriately trained, and experienced staff to successfully design and operate both the business and technical functions of the DE Component from contract execution through maintenance and operations.

A.12.2.3.1. The Contractor shall be required to provide a fully qualified, expert user with three (3) or more years of experience with the DE Component for TennCare and MMPVP training.

A.12.2.3.2. The Contractor shall provide adequate staff to support interpretation, guidance, and training to all TennCare approved users regarding reporting, analytics, and Dashboards.

A.12.2.4. The Contractor shall collaborate with TennCare and MMPVPs to develop and provide a Training Plan, for TennCare approval, that details all the activities required to efficiently, accurately, and effectively train all TennCare identified and approved personnel in the complete use and operation of the Contractor's DE Component in accordance with TennCare's training strategy. Once approved by TennCare, the Contractor is responsible for implementing the Training Plan, as written, revised, and approved by TennCare, to comply with all system and business operational standards and service levels of the enterprise wide solution over the life of the Contract.

A.12.2.4.1. The Contractor shall collaborate with TennCare and MMPVPs to develop a Training Plan that is tailored to specific user roles and groups. The Training Plan shall, at a minimum, addresses the following:

A.12.2.4.1.1. Descriptions of training solutions and knowledge transfer programs for both highly technical and non-technical users across the enterprise;

A.12.2.4.1.2. The inclusion and development of a system training environment;

A.12.2.4.1.3. Necessary hardware and/or software installations;

A.12.2.4.1.4. Providing a training location within fifteen (15) miles of TennCare's offices in the event existing office location does not meet training capacity needs;

A.12.2.4.1.5. Training curricula including, but not limited to, role-based training, users with varying levels of security access and administrations, to include business decisions and processes which integrate with system functionality;

A.12.2.4.1.6. The approach to and delivery of a train-the-trainer program;

A.12.2.4.1.7. Procedures for maintaining documentation for each functional area, screen layouts, report layouts, and other output definitions, including examples and content definitions;

A.12.2.4.1.8. The creation of training materials and job aids, including, but not limited to, user manuals, business rules, and all other documentation appropriate to the platform, operating systems, and programming languages;

A.12.2.4.1.9. Approach to providing the training necessary to support new functionalities or major system releases; and

A.12.2.4.1.10. Secondary/backup training plans to deliver remote or virtual training of equal substance and comprehensiveness in the event of a declaration of a state of emergency by the State or at the discretion of TennCare.

A.12.2.4.2. The Contractor shall collaborate with TennCare and MMPVPs to identify training needs, update the Training Plan and training materials for identified trainings, and submit the Training Plan for TennCare review and approval in an agile, ongoing, iterative process.

A.12.2.4.3. TennCare and MMPVPs reserve the right to direct the Contractor to amend or update its Training Plan at no additional cost to TennCare.

A.12.2.5. The Contractor shall collaborate with TennCare and MMPVPs to create and deliver training materials necessary to support training of TennCare staff and end-users, including the development of any necessary video tutorials, slides, instruction manuals, or other materials that will be used in training sessions.

A.12.2.5.1. The Contractor shall provide samples of training materials, knowledge transfer materials, and system documentation, such as user guides, to TennCare and MMPVPs for review and approval per training timelines defined in the SILC.

A.12.2.5.2. The Contractor shall create, review, and update training materials in an agile, ongoing, and iterative process as outlined by TennCare and MMPVPs. All materials shall be reviewed and updated by the Contractor as continued system releases or updates impact the effectiveness of the training materials or as deemed necessary by TennCare. All materials shall be approved by TennCare and MMPVPs prior to use.

A.12.2.5.3. The Contractor shall provide for accessible online help for enterprise Users when using the DE Component.

A.12.2.5.4. The Contractor shall collaborate with TennCare and MMPVPs to use TennCare-provided user feedback to shape training as defined by TennCare.

A.12.2.6. The Contractor shall provide a train-the-trainer session to TennCare identified stakeholders and MMPVPs on the execution of the Business Continuity Plan prior to implementation of the Contractor's DE Component, with the implementation of major changes, annually thereafter, or more frequently as directed by TennCare.

A.12.2.7. The Contractor shall provide ongoing training on the DE Component. Details on the ongoing training requirements will be determined by the Training Plan.

A.12.2.8. The Contractor shall utilize TennCare's enterprise learning management platform for the administration, documentation, tracking, reporting, and delivery of training programs for the Contractor's DE Component as directed by TennCare.

A.12.2.9. The Contractor shall adhere to utilizing a central training repository which will be identified by TennCare (i.e. enterprise learning management tool, SharePoint, Confluence, etc.) for all training materials which will archive training materials, track the history of changes/approvals, and allow for the retention of materials in accordance with TennCare defined data retention policies. All customized materials shall be the property of TennCare and shall be readily accessible and available on demand to TennCare.

A.12.2.10. The Contractor shall provide virtual and remote user training options as requested by TennCare.

A.12.2.11. The Contractor shall create a TennCare-approved security access and protocol training for internal and external DE Component users and maintain evidence of training completion prior to solution access privileges.

A.12.3. Staffing

A.12.3.1. General Staffing Requirements

A.12.3.1.1. All personnel shall be employees or contracted staff of the Contractor and fully qualified to perform the work required in this Contract. The Contractor shall provide experienced, qualified professionals to be present, focused, and engaged with TennCare and MMPVPs and to ensure the success of this project. The Contractor shall provide personnel in sufficient quantity to provide consistent and high-quality Deliverables and supporting work product, even during periods in which work on multiple projects are underway.

A.12.3.1.2. The Contractor work will normally occur during TennCare's core business hours (7:00 AM to 7:00 PM Central time, Monday through Friday), during which the Contractor must provide coverage of business areas as determined by TennCare. As directed by TennCare, exceptions may occur to accommodate scheduled project events that must occur during evenings or on weekends. Contractor will furnish Contractor personnel as needed for after-hours projects. Contractor work and travel schedules shall be approved in advance by TennCare's Program Director. The Contractor shall have production support staff available twenty-four (24) hours per day, seven (7) days per week during Operations and Maintenance.

A.12.3.1.3. Other than required approval of Key Personnel as detailed in A.12.4.8 and subcontractors by TennCare, the Contractor shall have the responsibility for hiring and management of all Contractor staff and subcontractors. The Contractor shall be responsible for maintaining a level of staffing necessary to perform and carry out all Services required by this Contract, regardless of the level of staffing included in its proposal. After consultations with the Contractor, TennCare shall make the final decision as to the required staffing levels based upon current progress in meeting the goals of the DE and DE Component and anticipated future needs for the DE and DE Component. TennCare will use the Control Memorandum process to indicate dates by which staffing increases or replacements must be made. Failure to meet the staffing deadlines in the Control Memorandum may lead to the imposition of Liquidated Damages as specified in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.12.3.1.4. The Contractor shall not use offshore staffing resources to perform any Services included in or provided pursuant to this Contract.

A.12.3.1.5. On-Site Staffing Requirements. "On-Site" shall mean that the indicated Contractor staff and/or subcontractors shall be physically present during the percentages identified in Section A.12.4.8 from their start date through the term of the Contract, until they are no longer performing Services under the Contract, or as otherwise approved by TennCare. Personnel are considered On-Site when working at either the Contractor's offices described in Section A.12.5.1 or at the TennCare offices located in Nashville, Tennessee. On-site positions also require the Contractor staff and/or subcontractors to meet the dedication requirements for each role. Percentage dedicated means that the personnel shall be assigned to work the required portion of their time on the Services provided under this Contract, and the personnel may not work full or part time on other work without TennCare's prior written approval.

A.12.3.1.5.1. At the direction of TennCare, the Contractor shall reduce or eliminate the On-Site percentages identified for Key Personnel in Section A.12.4.8 at any time during the Contract term.

A.12.3.1.6. The Contractor shall ensure that the roles that are established to support Operations and Maintenance and that are staffed shall be included in the measurement of Operations and Maintenance headcount for a given period, even though they may also be supporting enhancement activity for the same period.

A.12.3.1.7. TennCare shall have the discretion to approve or disapprove the Contractor's and any of its subcontractor's staff or to require the removal or reassignment of any of Contractor's or subcontractor's staff found unacceptable to TennCare for work under this Contract only.

A.12.3.1.8. The Contractor shall keep track of resource costs, both personnel and technical, on a per project basis in order to satisfy TennCare and CMS reporting requirements for enhanced federal funding assistance. These resource costs shall be maintained by the Contractor and provided to TennCare, upon request, to support all projects. After consultation with the Contractor, TennCare will approve an invoice format that will meet the needs of TennCare and CMS. The Contractor shall submit an invoice as required by Section C.5 for approval once TennCare has issued Acceptance of the Deliverable.

A.12.3.2. Subcontracted Staff

A.12.3.2.1. With regard to those subcontractors approved by TennCare during procurement of this Contract in accordance with Section D.7, the Contractor shall provide TennCare with a fully executed, complete copy of each subcontract on or before the earlier of: (a) such subcontractor beginning work on this Contract or (b) within thirty (30) days of execution of the Contract. With regard to subcontractors approved by TennCare and engaged by Contractor after the Contract start date, the Contractor shall provide TennCare with a fully executed, complete copy of each subcontract on or before the earlier to occur of: (a) such subcontractor beginning work on this Contract or (b) within thirty (30) days of TennCare's approval of the subcontract.

A.12.3.2.2. The Contractor shall not substitute a subcontractor for a subcontractor previously approved by TennCare without the prior written approval of TennCare, as required by D.7.

A.12.3.3. INENTIONALLY OMITTED.

A.12.4. Key Personnel

A.12.4.1. The term "Key Personnel" refers to Contractor personnel deemed by TennCare to be essential to the Contractor's satisfactory performance of the requirements contained in this Contract. Contract Section A.12.4.8. Table 2 – Key Personnel contains the required Key Personnel positions, corresponding roles and responsibilities, and minimum qualifications for each. If the scope of Services in this Contract includes all four (4) DE Components, the Contractor must provide a minimum of two (2) Key Personnel staff members for the following positions: Project Manager, Technical Manager, Testing Manager, and Security Lead. If the Contractor is providing two (2) or more DE Components, TennCare may, in its sole discretion, consolidate multiple personnel for a single Key Personnel position. The green shaded cells in Section A.12.4.8. Table 2 – Key Personnel indicate DE Component(s) that may be consolidated by one (1) individual in that Key Personnel position if the indicated DE Component(s) are awarded to the same Contractor.

A.12.4.1.1. All Key Personnel shall be employees of the Contractor or contracted staff of the Contractor and be present full-time at either the Contractor's office in Tennessee or at TennCare offices in Nashville, Tennessee as described in the Key Personnel Table, Table 2 below, or as otherwise approved by TennCare.

A.12.4.1.2. The Contractor shall obtain TennCare's prior written approval of all Key Personnel. The Contractor shall provide resumes for all Key Personnel toto TennCare at least thirty (30) days prior to the expected employee's start date on this Contract. TennCare reserves the right to conduct in-person interviews with Key Personnel prior to the Key Personnel's start date on this Contract. The Contractor may utilize the same personnel for more than one (1) Key Personnel position in different Gate Reviews with prior written approval from TennCare. The Contractor shall not make any changes to the proposed positions, staff, and responsibilities of Key Personnel without TennCare's prior written approval.

A.12.4.1.3. If the Contractor deems an additional Key Personnel position(s) necessary beyond the positions listed in Table 2 below, the Contractor shall identify these positions and provide a complete description of how these positions support the fulfillment of the Contract. All Key Personnel must be formally committed to join the project by the beginning of the Contract start date.

A.12.4.1.4. If any Key Personnel are not employees of the Contractor, the Contractor shall identify those personnel and provide TennCare with contracts establishing their subcontract. The Contractor shall not employ or use a subcontractor without the written approval of TennCare.

A.12.4.1.5. References for Key Personnel shall meet the following requirements:

A.12.4.1.5.1. A minimum of three (3) professional references outside the employee's current employer who can provide information about the Key Personnel's work on relevant past assignments;

A.12.4.1.5.2. The reference's full name, mailing address, telephone number, and e-mail address;

A.12.4.1.5.3. For any client contact listed as a reference, include the agency's or company's full name with the current telephone number and e-mail address of the client's responsible project administrator or service official who is directly familiar with the Key Personnel's performance;

A.12.4.1.5.4. The Key Personnel's professional experience within the past five (5) years; and

A.12.4.1.5.5. All professional certifications and affiliations.

A.12.4.2. Key Personnel resumes shall include the following information:

A.12.4.2.1. Employment history for all relevant and related experience;

A.12.4.2.2. Names of employers for the past five (5) years, including specific dates; and

A.12.4.2.3. All educations institutions attended and degrees obtained.

A.12.4.3. The Contractor shall provide guidance on the necessary steps to make staffing assignment changes. The Contractor shall also define procedures for Key Personnel transitions for TennCare approval.

A.12.4.4. TennCare retains the right to approve or disapprove proposed Key Personnel staffing and reserves the right to require the Contractor to replace specified staff. The Contractor shall substitute, with TennCare's prior approval, any employee so replaced with an employee of equal or better qualifications. The Contractor shall provide an interim employee within five (5) Business Days of any Key Personnel vacancy regardless of the reason for the vacancy. The Contractor shall propose a substitute employee within thirty (30) days, and the Contractor shall ensure that the substitute employee begins work for the Contractor within forty-five (45) days. If the Contractor does not provide Key Personnel in compliance with each of the three (3) stated timeframes, the Contractor will be assessed Liquidated Damages in accordance with Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL. In the event it becomes necessary to replace Key Personnel during the term of this Contract, the Contractor shall:

A.12.4.4.1. Provide TennCare's Program Director with written notification of such replacement, providing, when possible, for a two (2) week period for knowledge transfer from the Key Personnel to the replacement personnel. This knowledge transfer shall be provided at no charge to TennCare;

A.12.4.4.2. Provide TennCare's Program Director with documentation describing the circumstances of the need for the replacement;

A.12.4.4.3. Provide documentation of experience for the proposed replacement personnel;

A.12.4.4.4. Obtain prior written approval from TennCare's Program Director; and

A.12.4.4.5. During the first twelve (12) months of the Contract performance period, no substitutions of Key Personnel shall be permitted unless such substitutions are necessitated by an individual's sudden illness, death, or resignation, or otherwise approved by TennCare's Program Director or requested by TennCare. In any of these events, the Contractor shall follow the steps outlined in this Section. Failure to meet the prior notice and approval requirements herein may result in the imposition of Liquidated Damages as contained in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.12.4.5. Staffing Needs Planning and Monitoring Processes

A.12.4.5.1. The Contractor shall provide an overview report of the preliminary and ongoing staff planning and monitoring processes at a frequency determined by TennCare. The report shall specifically identify activities for planning for future needs and monitoring of the project assignments, contract timelines, the nature of existing and anticipated vacancies,

length of time a position has been vacant, status of hiring, and associated decisions for release or renewal of personnel.

A.12.4.6. Turnover Staffing

A.12.4.6.1. The Contractor shall provide a full-time turnover manager as a designated point person to interact with TennCare and a successor contractor until Contract Term is completed.

A.12.4.6.2. The Contractor shall provide and retain sufficient Key Personnel resources, if applicable, during Turnover, inclusive of technical staff (e.g. systems analysts, technicians) and non-technical staff (e.g. clerical staff, business analysts) resources to complete the Services and meet the requirements specified in the Contract.

A.12.4.6.3. The Contractor shall include staffing for operations during Turnover in the Staffing Management Plan.

A.12.4.7. Off-Boarding

A.12.4.7.1. The Contractor shall appoint a Contractor Liaison who is responsible for completing an off-boarding request in the ITSM tool within twenty-four (24) hours of a resource departure.

A.12.4.7.2. In the event of a resource departure, the Contractor shall provide prior notification, with appropriate forms to TennCare's Access Management team and appropriate TennCare management staff in advance of termination, if known, or immediately after the resource submits their resignation.

A.12.4.8. Key Personnel Table. The cells marked with "x" are required Key Personnel positions for the applicable DE Component. The green shaded cells in the table below indicate DE Component(s) that may be consolidated by one (1) individual in that Key Personnel position, if the indicated DE Component(s) are awarded to the same Contractor.

TABLE 2: KEY PERSONNEL TABLE

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
Account Manager	The Account Manager will serve as the primary Contractor point of contact for activities related to contract administration, project management, scheduling, resource management, correspondence with TennCare's leadership, and Deliverable reviews.	• A minimum of eight (8) years of experience in managing and leading a large-scale or enterprise-wide healthcare IT systems contract or project that encompasses a full software development lifecycle from initiation through post-implementation and includes operations and maintenance; • A minimum of five (5) years of experience serving in an account management or client representative position; • Subject matter expertise on relevant State and Federal Medicaid regulations and policies; and • Previous experience following a standard project management methodology and in using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources.	• Shall not serve in any other position; • Shall be On-site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-site during the Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x	x	x	x
Project Manager	The Project Manager, in collaboration with the TennCare Project Manager, is responsible for planning, directing, managing, and overseeing the overall Contractor project management activities. The primary focus is on providing an integrated view of all project and related program activities.	• A minimum of five (5) years of experience leading a large scale or enterprise-wide healthcare IT systems contract or implementation; • A minimum of ten (10) years of experience managing IT systems programs and/or projects; • Previous experience following a standard project management methodology and in using various	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare;	x	x	x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		project management tools in developing project plans, delivering tasks, and tracking timelines and resources; and • Preferred PMP certification.	• Shall be On-Site during the Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.				
Technical Manager	The Technical Manager will serve as the primary point of contact with TennCare's Technical Staff. The Technical Manager will serve as the technical subject matter expert and Solution Architect over the Contractor's team. The Technical Manager will lead the strategy and implementation for the end-to-end Solution by taking into consideration TennCare's business case, objectives, requirements, constraints, technology landscape, and technology standards.	• A minimum of eight (8) years of experience implementing large-scale healthcare IT solutions within environments similar to that of the MMIS; • A minimum of ten (10) years of experience building and supporting mission critical, multi-tier large scale healthcare applications; • Shall be familiar with Data Governance concepts like Metadata Management and Master/Reference Data Management; • Possess extensive experience architecting multi-tier platforms that employ SOA; • Possess extensive experience utilizing SOA patterns, automating business process models, and employing cloud-based services; • Shall be knowledgeable of secure coding practices; • Shall possess MITA experience; • Experience with technical requirements for data classifications and implementing data protection technologies; • Must possess extensive experience developing solutions utilizing an	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x	x	x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		integrated development environment, multi-tier platforms, and employing SOA architecture with high availability/reliability requirements; • Must be proficient in multiple languages, SOA technologies, operating systems, and security best practices; • Possess expert knowledge of the Contractor's DE Component, having implemented a comparable solution to the DE Component in no less than one (1) environment at least as complex as the MMIS; and • Experience implementing data warehouse solutions within an integrated environment and employing SOA and intelligent business reporting.					
Certification Manager	The Certification Manager shall be the contact for the TennCare certification team in its engagement and interaction with CMS for certification efforts for the DE. The Certification Manager shall ensure the DE Component functionality and business operations meet the requirements to achieve CMS Certification. The Certification Manager will need to be able to support the certification mechanism required by CMS at the time of certification. The Certification Manager shall develop and implement a strategy and plan for proper documentation of system Artifacts to support the DE certification process. The Certification Manager will provide oversight and coordination of the DE certification process, prepare for, and lead the TennCare participation in periodic certification reviews.	• Shall possess at least five (5) years of similar CMS Certification experience.	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase seventy-five (75%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x	x	x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
Operations and Maintenance (O&M) Manager	The O&M Manager is responsible for system operations and ongoing maintenance after the DDI and the Module Integration implementation. The O&M Manager serves as the point-person for all Contract management, Contract performance management, and escalations. The O&M Manager provides Contract performance and SLA support to TennCare as defined throughout this Contract. The O&M Manager will serve as the lead on service management areas of the Contract.	• Shall possess at least five (5) years of similar O&M experience; • Previous experience in maintaining and adhering to Service Level Agreement requirements; • A minimum of seven (7) years of experience in the service management aspects of the solution, including, but not limited to, change management, Incident Management, risk evaluation, and Problem Management; and • A minimum of seven (7) years of experience on technical aspects of solutions, including, but not limited to, infrastructure, application, and data warehousing.	• Shall not serve in any other position; • Shall be On-Site during DDI twenty-five percent (25%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x	x	x	x
Security Lead	The Security Lead is responsible for the assessment, planning, and implementation of all security standards, practices, and components required for the DE Component implementation. The Security Lead is responsible for adherence to TennCare security standards, communications with TennCare CISO, compliance with HIPAA, HITECH, NIST requirements, and IRS FTI.	• Minimum of five (5) years related experience in a large-scale mission critical environment; • Must be familiar with at least one (1) major security compliance framework and be able to demonstrate a firm understanding of relevant State and Federal security/privacy regulations and policies, specifically under NIST, HIPAA, and IRS Pub. 1075; • Must have successfully guided security compliance on at least one (1) project with similar size and scope; • At least one (1) relevant professional information security certification required: CISSP, CISM,	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed	x	x	x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		CRISC, SANS, GIAC, or similar; and • Extensive experience dealing with Sensitive Data information systems.	upon with TennCare; and • Shall be available as needed post Go-Live.				
Testing Manager	The Testing Manager will perform and provide technical leadership for test activities to include planning, execution, and reporting.	• Possess a minimum of seven (7) years of experience managing testing functionality similar to the Contractor's DE Component; • Possess a minimum of five (5) years of experience developing and executing testing scenarios for solutions similar to Contractor's DE Component; • Possess a working knowledge of the Contractor's DE Component; • Possess a working knowledge of business processes associated with the DE; and • Possess a working knowledge of performance and load testing.	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x	x	x	x
Cloud Manager	The Cloud Manager is responsible for defining and documenting network, security server, SOA, and the operating system specifications for the DE Component. The Cloud Manager will also be responsible for translating the infrastructure requirements to the DE Component.	• Possess a minimum of seven (7) years of experience in infrastructure and systems design; • Possess a minimum of five (5) years of direct experience configuring, operating, and maintaining cloud environments; • Possess a minimum of three (3) years of experience managing projects of similar size and complexity; • Possess a minimum of three (3) years of experience in managing state level projects, either having	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations &	x	x	x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		delivered projects to a state or worked in a state government delivering Health and Human Services related projects; • Expert understanding of operating system(s) that the DE Component is running; • Strong understanding of load balancing (F5 LTM & GT preferred); • Solid understanding of internet access using a Demilitarized Zone (DMZ) for things such as, but not limited to, proxies, web servers, firewalls, DNS, and certificates; and • Knowledge of complex network routing.	Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.				
Business Architect	The Business Architect leads the development of the business requirements and needs assessment for a DE Component project and architecting a clear business solution. The Business Architect works with the data and delivery teams to ensure that the DE Component design will meet business needs. The Business Architect works with the business teams to ensure that changes to process design and workflow are addressed as part of the overall solution. The Business Architect is responsible for developing the functional specification and support development and testing as needed.	• A minimum of eight (8) years of experience implementing large-scale healthcare IT solutions within environments similar to that of the MMIS; • A minimum of ten (10) years of experience building and supporting mission critical, multi-tier large scale healthcare applications; • Possess a working knowledge of business process modeling; • Possess expert knowledge of the Contractor's DE Component, having implemented a solution similar to the DE Component in no less than one (1) environment at least as complex as the MMIS; • Possess expert knowledge of national policy and standards that impact the Medicaid environment; • Possess generalized knowledge of data structures, Data modeling, and data configurations; and • Possess experience with Metadata management.	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.		x	x	

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
Data Architect	The primary role of the Data Architect is to lead the strategy and implementation for the data integration solution. The technical domain of the Data Architect includes conceptual, logical, and physical Data modeling, data integration standards, source to target mapping, best practices, tools and technologies, security in the data integration environment, data integration architecture, design, development, capacity planning, performance tuning, and administration.	• A minimum of five (5) years of experience developing and implementing one (1) or more Industry Standard Database systems; • Capable of hands-on work in all phases of Database design and management; • Significant experience managing operational Databases including handling complex migrations with mission critical applications; • Extensive experience dealing with Sensitive Data and healthcare Industry Standards and regulations; • Experience with technical requirements for data classification and implementing data protection technologies; and • Must be knowledgeable of secure coding practices for Databases.	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x		x	x
ETL Manager	The primary role of the ETL Manager is to oversee the development and implementation of the ETL process based on TennCare's needs.	• A minimum of five (5) years of experience with ETL development or Data modeling; • Broad knowledge of Database administration tool sets; • Experience with Database software installation, upgrades, management, troubleshooting, design, support, including backups and recovery, data migration techniques, and Database security; • Extensive experience using and tuning SQL; • Minimum of five (5) years of experience managing complex conversion projects from disparate Legacy Databases into different Data Models;	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed			x	

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		• Minimum of five (5) years of experience designing, programming, administering, and tuning complex conversions that move data from multiple disparate Legacy Databases into separate/different Data Models; • Must have experience with the Contractor's chosen ETL/conversion toolset with at least two (2) prior conversions; • Experience with managing and documenting conversion efforts and staff; and • Experience with writing, testing, configuring, and tuning conversion code.	upon with TennCare; and • Shall be available as needed post Go-Live.				
Database Administrator	The primary role of the Database Administration (DBA) is designing, developing, and implementing infrastructure to provide highly complex, reliable, and scalable Databases to meet TennCare's objectives and requirements. The DBA shall maintain Database performance by calculating optimum values for Database parameters, implementing new releases, completing maintenance requirements, and evaluating computer operating systems and hardware products.	• Minimum of seven (7) years of experience managing a complex relational database management system environment on a UNIX platform with multiple environments (development, test, production, etc.); • Broad knowledge of Database administration toolsets; • Experience with Database software installation, upgrades, management, troubleshooting, design, support (including backups and recovery), data migration techniques, and Database security; • Extensive experience using and tuning SQL; • Experience with Database conversions from disparate systems(s); • Capable of hands-on work in all phases of Database design and management; • Significant experience managing operational Databases including handling complex migrations with mission critical applications;	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live.	x		x	x

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
		• Extensive experience dealing with Sensitive Data and healthcare Industry Standards and regulations; • Experience with technical requirements for data classification and implementing data protection technologies; and • Must be knowledgeable of secure coding practices for Databases.					
Module Support Manager	The Module Support Manager is responsible for reporting KPIs, Module Support, and SLAs.	• A minimum of five (5) years of managing and reporting on Service Level Agreements; • A minimum of five (5) years of reporting on KPI metrics; • A minimum of three (3) years of managing performance outcomes for system upgrades; • A minimum of three (3) years of experience managing projects of similar size and complexity; • A minimum of three (3) years of experience managing and reporting on incident tickets; • Extensive knowledge of Contractor's DE Component(s); and • Working or general knowledge of other DE Component(s), if any.	• Shall not serve in any other position; • Shall be On-Site seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; and • Shall be On-Site during Operations & Maintenance Phase seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare.	X	X	X	X
Project Scheduler	The Project Scheduler will serve as the primary contact for all schedule-related items throughout the duration of the Contract. The Project Scheduler will work directly with the TennCare PMO, SPMO, and DE Component PMO to ensure that the DE Component schedule is developed, updated, and maintained in alignment with the cadence and process established for the program. Additionally, the Project Scheduler will identify any dependencies with other solution vendors and will work with the SPMO Master	• A minimum of five (5) years of experience in managing the program and/or project schedules for a large-scale or enterprise-wide IT systems contract or program and/or project that encompasses a full software development lifecycle from initiation through post-implementation; • Possess extensive experience in developing and maintaining project timelines for large-scale IT solutions;	• Shall not serve in any other position; • Shall be On-Site during DDI seventy-five percent (75%) of the time, unless otherwise agreed upon with TennCare; • Shall be On-Site during the	X	X	X	X

Key Positions	Description	Minimum Qualification	Requirements	EDW	DSS	DQ/ ETL	MDM
	Scheduler to ensure they are implemented accurately into the Integrated Master Schedule.	• Previous experience following a standard project management methodology and in using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources; • Working knowledge of Project Scheduling software's such as Microsoft Project 2013 (or later), Microsoft Project Server, and Microsoft Excel; and • Preferred PMP Certification.	Operations & Maintenance Phase fifty percent (50%) of the time, unless otherwise agreed upon with TennCare; and • Shall be available as needed post Go-Live. •				

A.12.5. Facility

A.12.5.1. The Contractor shall secure a temporary office space within six (6) weeks of the start of the Contract. At the end of the six (6) week period, the Contractor shall have another six (6) weeks to secure a permanent facility sufficient to house its staff to fulfill the entire scope of this Contract. The facility shall be located within a fifteen (15) mile radius of the TennCare office located at 310 Great Circle Road, Nashville, TN or other permanent address of TennCare, as designated by TennCare. The Contractor shall either directly house all necessary subcontractors or otherwise ensure the availability of necessary subcontractors to successfully complete the requirements of this Section. If applicable, TennCare recommends that Contractor(s) providing the DE Component of the DE Solution are co-located within five (5) miles of one another.

A.12.5.2. TennCare may require certain Contractor personnel, as determined by TennCare, to work On-Site at TennCare offices at any point in the Contract, including during the time before the Contractor's temporary office space is secured.

A.12.5.3. The Contractor staff shall be available for meetings at the TennCare office and at the Contractor's local office as determined by TennCare. The Contractor shall meet with TennCare's offices or the Contractor's local offices, as determined by TennCare. Whenever appropriate meeting space is available at the TennCare office, the meetings shall be held at TennCare's offices. Should appropriate meeting space in TennCare's preferred office(s) be unavailable, the Contractor shall provide an appropriate meeting space.

A.12.5.4. The Contractor shall adhere to TennCare guidelines regarding health and safety while On-Site at the TennCare office.

A.12.5.5. The Contractor shall leverage TennCare's video conferencing and collaboration licenses and tools (e.g. WebEx, Cisco TelePresence MX300 G2, and MX200 G2, etc.), where possible. Meetings shall be held remotely at the sole discretion of TennCare.

A.12.5.5.1. If the Contractor does not leverage TennCare's existing video conferencing and collaboration license or tools, the Contractor shall provide TennCare with licenses for a TennCare-approved Industry Standard teleconferencing service to allow for remote meetings at no additional cost to TennCare.

A.12.5.6. The Contractor shall provide dedicated spaces at the Contractor's off-site local office location for a minimum of ten (10) and a maximum of twenty (20) full time TennCare staff and MMPVPs to be collocated with the Contractor and provide additional hoteling spaces as needed.

A.12.5.6.1. The Contractor shall provide parking locations for TennCare staff and MMPVPs at no cost to TennCare.

A.12.5.7. The Contractor shall accommodate project activities at the Contractor's off-site local office location, including, but not limited to, the following:

A.12.5.7.1. Contract administration/housing key personnel;

A.12.5.7.2. Project Coordination, Joint application design (JAD) and review sessions;

A.12.5.7.3. Demonstrations of design prototypes;

A.12.5.7.4. Discussion and presentations of proposed system design changes;

A.12.5.7.5. Deliverable walkthroughs;

A.12.5.7.6. Technical and user support Service Desk functions;

A.12.5.7.7. System testing task walkthroughs;

A.12.5.7.8. User Acceptance Test support;

A.12.5.7.9. Implementation planning;

A.12.5.7.10. Transition management support; and

A.12.5.7.11. Regularly scheduled and TennCare-requested training sessions.

A.12.5.8. The Contractor shall collaborate with TennCare to provide a Facilities Management Plan for TennCare approval that, at a minimum, addresses the facility challenges presented within a multi-contractor, integrated solution. The Contractor shall notify TennCare of any changes in the plan at least twenty (20) Business Days prior to the change.

A.12.5.9. The Contractor shall not permit the Contractor's employees, agents, representatives, or subcontractors to share, store, access, use, transport, or disclose TennCare data in any form via any medium, including with any third parties, beyond the boundaries and jurisdiction of the United States of America without express written authorization from TennCare.

A.12.5.10. The Contractor shall not allow the Contractor's employees, agents, representatives, or sub-contractors to perform DDI or O&M activities on the DE Component beyond the boundaries and jurisdiction of the United States or to leverage systems infrastructure, components, or resources that are hosted beyond the boundaries and jurisdiction of the United States in support of these activities without the express written authorization from TennCare.

A.12.5.11. The Contractor shall ensure that all facilities supporting this Contract are protected against threats, during working and non-working hours, with an appropriate surveillance alarm/system extended to a manned monitoring system extended to a manned monitoring center, and adhere to IRS SCSEM, CMS MARS-E, SSA, and TennCare security framework.

A.12.5.12. The Contractor shall deliver equivalent Service performance via enhanced use of teleconferencing, collaboration, and workflow tools to fulfill all requirements of this Contract at TennCare's request.

A.12.6. Warranty

A.12.6.1. The Contractor represents and warrants that the term of the "Warranty Period" for the DE Components shall be the greater of the Term of this Contract or any other warranty generally offered by Contractor, its suppliers, or manufacturers to customers of its good or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge. Incidents and Problems identified during the Warranty Period may be considered Defects as determined by TennCare.

A.12.6.2. The Contractor represents and warrants that TennCare is authorized to possess and use all equipment, materials, software, and Deliverables provided under this Contract.

A.12.6.3. The Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

A.12.6.4. If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then TennCare shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of TennCare's rights under this Section shall not prejudice TennCare's rights to seek any other remedies available under this Contract or applicable law.

A.12.6.5. The Contractor represents and warrants that each release of the DE Component will conform to system requirements and expected outcomes as detailed in the functional design documentation, technical design documentation, and TennCare System Security Plan (SSP) Template as approved by TennCare.

A.12.6.5.1. The Warranty Period shall begin only after the resolution of all Defects identified prior to the Go-Live of that release.

A.12.6.6. The Contractor represents and warrants that each subsequent DE Component release will build upon and conform to previously released functionality, unless a change is explicitly approved by TennCare.

A.12.6.7. In the event that a subsequent release creates or identifies Defects in the deployed DE Component, the Warranty Period of the created or identified Defect will be covered by the Warranty of that subsequent release.

A.12.6.8. If the Contractor will perform Warranty work after Turnover of the DE Component, the Contractor shall include Warranty Deliverables, testing, and any additional documentation requested by TennCare as part of the Turnover Plan.

A.12.6.9. Documentation and Resolution of Warranty Defects

A.12.6.9.1. The Contractor shall classify Warranty Defects as severity level low, medium, high, and critical as described in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL and track Defects as required in Section A.12.6 of this Contract.

A.12.6.9.2. The identification of critical and high Defects of the DE Component during the Warranty Period shall extend the Warranty Period for DE Component for six (6) months after the time of the resolution of critical or high Defects.

A.12.6.9.3. The Contractor shall be responsible to resolve all critical and high Warranty Defects within the periods described in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, or, if necessary, provide TennCare with a mutually acceptable written work-around, downstream impacts, and plan for resolution, all without additional cost to TennCare.

A.12.6.9.4. The Contractor shall resolve all medium and low Defects within the periods described in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.12.6.9.5. The Contractor shall be subject to corresponding Liquidated Damages, listed in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, for all identified Warranty Defects that are not resolved within the associated resolution timeframes.

A.12.7. Change Order – Special Projects & Enhancements

A.12.7.1. Special Projects or Enhancements are additional projects that TennCare may, at its sole discretion, initiate and assign to the Contractor during the DDI or O&M phase of the Contract for the performance of services, fulfillment of

additional requirements, or creation of Deliverables or Services that are within the Scope of this Contract but were inadvertently unspecified.

A.12.7.2. A Special Projects fund and Enhancement fund will be created for each DE Component.

A.12.7.3. Changes Orders for each Special Project or Enhancement shall be implemented by a Control Memorandum as described in A.12.8.

A.12.7.4. Support Change Requests

A.12.7.4.1. The Contractor shall review Business Services Definitions issued by CMS and provide TennCare with a solution impact analysis on requirements and interfaces within seven (7) calendar days of receipt of a Change Request.

A.12.7.4.2. The Contractor shall perform impact analysis on Change Requests to identify impacts across business processes and business rules.

A.12.7.4.3. The Contractor shall perform risk analysis on Change Requests to identify risks and potential mitigations associated with development and deployment of the change.

A.12.7.4.4. The Contractor shall perform alternatives analysis for Change Requests to support the Medicaid Modernization Project Steering Committee (Project Steering Committee) with relevant information concerning alternative approaches to addressing the business need underlying the request.

A.12.7.4.5. The Contractor shall perform cost analysis for Change Requests as part of the Change Order process described in Section A.12.7. All Change Requests shall indicate implementation and full lifecycle costs for the proposed change.

A.12.7.4.6. The Contractor shall work with TennCare management to identify the impact of human resource costs as well as cross-project impacts associated with fulfilling the Change Request.

A.12.7.4.7. The Contractor shall provide analysis to support timing decisions for deployment of Change Requests in compliance with TennCare's release management process.

A.12.7.5. Change Order Creation

A.12.7.5.1. After receipt of a written request for the performance of Services, the Contractor shall respond to TennCare, within ten (10) Business Days, with a written proposal for completing the Services to fulfill TennCare's request for Services in a cost-effective manner. Contractor's proposal must specify:

A.12.7.5.1.1. The effect, if any, of implementing the requested change(s) on all other services required under this Contract. The Contractor shall provide TennCare, in writing, a listing of all anticipated or perceived impacts to the Contractor's DE Component and any integrating DE Component, to include the written impact specifications of the corresponding DE Component Contractor;

A.12.7.5.1.2. A description of the units of service needed to complete the change(s);

A.12.7.5.1.3. The specific effort involved in completing the change(s);

A.12.7.5.1.4. The expected schedule for completing the change(s);

A.12.7.5.1.5. The maximum number of person hours required for the change(s); and

A.12.7.5.1.6. A fixed price for all change(s) under the Change Order based on the Contractor's rate card as detailed in this Contract. The maximum cost for the Services shall in no instance exceed the product of the person hours required multiplied by the appropriate Payment rate proposed for such work.

A.12.7.6. The Contractor shall not perform any Services under the Change Order until TennCare has approved the Change Order proposal through a Control Memorandum(CM) containing a Control Directive that is signed by both TennCare and the Contractor. If approved, the CM and Change Order shall constitute a binding agreement between the Parties pertaining to the specified change(s) and shall, under this provision, be incorporated into this Contract by reference. All terms of this Contract, including, but not limited to Warranty, Service Level Agreements, and Liquidated Damages shall apply to Services provided under Change Orders.

A.12.7.7. Subsequent to creation of a Change Order, the Contractor shall complete the required Services. TennCare shall be the sole judge of the acceptable completion of Services and, upon such determination, TennCare shall provide the Contractor written approval.

A.12.7.8. TennCare will remunerate the Contractor only for work TennCare deems acceptable. All acceptable work performed pursuant to an approved Change Order shall be remunerated in accordance with Contract Section C.3. PROVIDED THAT, TennCare shall be liable to the Contractor only for the actual cost of the goods or Services completed, not to exceed the maximum cost for the change detailed in the Change Order. In no instance shall TennCare be liable to the Contractor for any amount exceeding the maximum cost specified by the Change Order. Upon TennCare approval of the work, the Contractor shall invoice TennCare in accordance with Section C.3.

A.12.8. Control Memorandum Process

A.12.8.1. The Control Memorandum (CM) process shall be utilized by TennCare to clarify Contract requirements, issue instruction to the Contractor, document action required of the Contractor, or request information from the Contractor. In addition, the CM process shall be used by TennCare to impose assessments of damages, either actual or liquidated. This process will be used to address issues or matters that do not require a contract amendment. Each CM must be in writing and indicate the date on which it was issued. CMs may provide relevant history, background, and other pertinent information regarding the issue(s) being addressed in the CM. Each CM will establish a deadline or timeframe for the Contractor's reply or other action. All CMs submitted to the Contractor must be signed and approved by TennCare's Project Director (or his/her designee). When the CM pertains to damages, either actual or liquidated, TennCare may issue consecutive CMs, as may be necessary or appropriate.

A.12.8.2. A CM may include one (1) or more of the following five (5) components of the CM process described below:

A.12.8.2.1. On Request Report – a request directing the Contractor to provide information by the time and date set out in the CM;

A.12.8.2.2. Control Directive (CD) – instructions that require the Contractor to complete, within a designated timeframe, one (1) or more Deliverables or to perform any other request from TennCare that is within the scope of the Contract. A CD may also provide clarification of certain Contract terms. Once a CM/CD has been issued, it shall be considered to be incorporated into this Contract;

A.12.8.2.3. Notice of Potential Damages (Actual or Liquidated) (NPD) – notification to the Contractor that TennCare has determined that a potential Contract performance or compliance issue exists and that TennCare is contemplating assessing damages, actual and/or liquidated. The NPD shall identify the Contract provision(s) on which TennCare's determination rests;

A.12.8.2.4. Notice of Calculation of Potential Damages (Actual or Liquidated) (NCPD) – notification to the Contractor that provides a calculation of the amount of potential damages, actual and/or liquidated, that TennCare is contemplating assessing against the Contractor. NPDs and NPCDs may be issued consecutively or simultaneously; or

A.12.8.2.5. Notice of Intent to Assess Damages (Actual or Liquidated) (NIAD) – notification to the Contractor that TennCare is assessing damages and specifying whether the damages are actual damages or Liquidated Damages and setting out the performance or compliance issue underlying each intended damage assessment. The NIAD shall identify the NPD and NCPD upon which it is based. The NIAD shall specify the total amount and type of damages, whether actual or liquidated, TennCare intends to assess. Following the issuance of an NIAD, TennCare may elect to withhold damages from Payments due to Contractor. TennCare may not issue a NIAD without first issuing an NPD and a NPCD. TennCare may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

A.12.8.3. Damages for failure to comply with CM. The Contractor shall fully comply with all CMs, compliance to be determined in TennCare's sole discretion. Failure to do so may result in TennCare pursuing recovery of damages, as defined in Contract Section E.10., including Liquidated Damages as listed in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL, a corrective action plan approved by TennCare, and/or termination of the Contract.

A.12.8.4. Appeal of Damages by Contractor. Contractor may appeal either the basis for NPD or calculation of NCPD potential damages, either actual or liquidated. To do so, the Contractor shall submit to the TennCare's Project Director (or his/her designee) a written response to the NPD and/or NCPD within ten (10) Business Days of receipt of a CM which includes an NPD or a NCPD. TennCare's Project Director (or his/her designee) shall review the appeal and provide notice of his/her determination to the Contractor through a CM. If the Contractor disagrees with TennCare's Project Director's (or his/her designee) initial appeal determination or TennCare's Project Director (or his/her designee) is unable to resolve the appeal, the Contractor may submit a written request to TennCare's Project Director (or his/her designee) that the matter be escalated to senior management of TennCare. Contractor shall submit such a request for escalation within ten (10) Business Days of its receipt of the initial appeal determination from TennCare's Project Director (or his/her designee) or of notification by TennCare's Project Director that he/she is unable to resolve the appeal. TennCare's senior management shall provide written notice of its final determination to the Contractor within (10) days of the receipt of the appeal from the Contractor. Upon appeal or escalation, TennCare shall not increase the amount of the potential damages.

A.12.8.5. Implement Corrective Action Plan. At TennCare's discretion, TennCare may, through a CM and Control Directive, issue a notice to the Contractor of its intention to impose a Corrective Action Plan (CAP) with the CM, accompanied by a request that the Contractor develop and propose an appropriate CAP for review and approval by TennCare within ten (10) days. TennCare shall determine the severity of the error using the critical, high, and medium

incident definitions as set forth in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL.

A.12.8.5.1. TennCare may, in its sole discretion, assess Liquidated Damages as set forth in the Liquidated Damages table located in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL. Each CAP shall, at a minimum, contain the following information:

i. Written documentation that includes acknowledgment of receipt of TennCare notice;

ii. Number of impacted Members and cases and such other information as TennCare may request;

iii. A description of how the Contractor has addressed or will address the immediate Problem;

iv. An analysis of the root cause of the Problem; and

v. A description of how the Contractor shall resolve the Problem (or has resolved the Problem) and shall prevent the Problem from recurring.

A.12.8.5.2. Upon acceptance of the CAP by TennCare, the Contractor shall be responsible for executing the CAP, and the CAP shall be incorporated by reference as part of this Contract. TennCare may request changes and/or additions to an approved CAP as deemed necessary to correct or resolve the Problems that led to requesting a CAP. The Contractor shall continue to comply with an approved CAP until TennCare notifies the Contractor, in writing, that all Problems outlined in the CAP have been satisfactorily resolved.

A.12.8.5.3. The Contractor shall be responsible for ensuring that all of its subcontractors or service providers comply with all approved CAPs. The Contractor shall be responsible for ensuring that all of its subcontractors or service providers comply with all approved CAPs.

A.13. Table of Deliverables

A.13.1. The Contractor shall refer to the TennCare Solution Implementation RACI and Deliverables of the TennCare Solution Implementation Lifecycle for the minimum requirements of the Contractor Deliverables during the Phased Implementation of the DE Component and Operational activities.

A.13.2. The Contractor shall complete the Deliverables identified throughout the lifecycle phases of the TennCare Solution Implementation Lifecycle and TennCare Solution Implementation RACI and Deliverables, as indicated in A.11 above. The TennCare Solution Implementation Lifecycle Document is organized into Phases and Gates with associated Deliverables that must be completed by Contractor and approved by TennCare. All Deliverables completed by Contractor and approved by TennCare shall be incorporated into this Contract. The TennCare Solution Implementation RACI and Deliverables Table of Deliverables is included below as Table 3: Table of Deliverables for reference purposes only.

A.13.3. The Contractor shall ensure Deliverables also comply with the corresponding TennCare standards documentation, located in Attachment C, Procurement Library, where applicable.

TABLE 3: TABLE OF DELIVERABLES

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Concept Requirements Review	Architecture Review Requirements Review	1. Project Management Plan	Baseline for project. High level PMP is initially approved during Concept phase and updated and approved again once the Solution Vendor is on-boarded during Requirements Review. Contains: 1. Scope 2. Schedule 3. Cost 4. Quality 5. Staffing/resource management (includes Vendor Organization Charts when updated after Vendor On-Boarding), and hardware and software requirements 6. Stakeholder register 7. Communications 8. Status reports 9. Processes and standards to manage risks, issues, assumptions, action items, and constraints 10. Capacity planning 11. Once Solution Vendor is on-boarded, determine Bill of Materials, including key acquisition-related activities and items (e.g., costs for hardware, software, and service acquisitions).	Validation that: 1. The submitted Project Management Plan and all sub-plans listed below address all components of each of the TennCare Project Management Plan and sub-plan templates in alignment with PMBOK standards: a. Communication Management Plan b. Decision Management Plan c. Document Management Plan d. Human Resource Management Plan e. Quality Management Plan f. Risk Management Plan g. Issue Management Plan h. Schedule Management Plan i. Scope Management Plan.	Type B
Concept Requirements Review Development	Architecture Review Requirements Review Validation Readiness Review	2. Implementation Schedule	The Implementation Schedule will be continually updated throughout project lifecycle. High level plan is initially approved during Concept phase, updated and approved again once the Solution Vendor is on-boarded during Requirements Review, and then once more before implementation go-live with the Implementation Plan.	Validation that the Implementation Plan: 1. Aligns with all Schedule Management Standards described in the TennCare Project Management Plan Standard 2. Is developed in Microsoft Project.	Type A
Concept Test	Architecture Review Implementation Readiness Review	3. Project Concept of Operations	Defines the project scope and target state architecture. Initially delivered during the Concept phase, then updated and approved again before Implementation. Contains: 1. Conceptual functions and stakeholder interactions 2. Scope Definition 3. Current System 4. Goals Objectives and Rationale for new or significantly modified system 5. Scenarios Analysis 6. Proposed System 7. Analysis of Proposed System 8. Business Requirements	Validation that: 1. Defines the target state architecture for the business need. This defines the project scope and boundary 2. Is aligned with CMS Standards and Conditions 3. Is aligned with the MITA State Self-Assessment and Roadmap to ensure that the project is advancing the capabilities of the business against the roadmap	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			May contain the following artifacts defined in the EA Modeling Standard: Business Goals, Value Logic Model, Business Service Model, Capability Model, Context Model, Business Function Model, Business Process Model, Business Scenarios, Stakeholder Model, Business Operating Model, Semantic Model, Conceptual Data Model, Application Component Model, Alternatives Analysis, Conceptual Integration Architecture, Volume and Performance Expectations.	4. Contains outcomes that are aligned with TennCare's target Enterprise Architecture 5. Considers all applicable security and privacy standards in sufficient detail 6. Does not duplicate, interfere, or contradict other efforts.	
Requirements Review	Requirements Review	4. Requirements Management Plan	Contains approach and methodology that the Solution Vendor will follow during the project lifecycle for managing requirements. This plan addresses how the Solution Vendor will manage missing requirements identified during the detailed requirements review.	Validation that: 1. The Requirements Management Plan are in alignment with TennCare Standards.	Type C
Requirements Review	Requirements Review	5. Requirements Traceability Matrix (RTM)	The RTM contains the initial solution requirements as published in the RFP for a Solution Vendor. It is updated throughout the lifecycle of the project.	Validation that: 1. The requirements in the RTM continue to align to TennCare's target state enterprise architecture and requirements as published in the RFP for a Solution Vendor 2. Once the Solution Vendor is on-boarded, requirements are elaborated to a level of detail that is testable, with defined acceptance criteria. 3. The RTM approved at the Requirements Review Gate must have project level solution requirements traced to the original contract requirements and to any CMS compliance criteria that are required for certification activities.	Type A
Requirements Review	Requirements Review	6. Risk Register / Exception Plan	List of project risks and mitigation plans for each. Completed by the Solution Vendor during on-boarding.	Validation that: 1. The project risks as outlined by the Solution Vendor are complete and accurate.	Type A
Requirements Review	Requirements Review	7. Certification Plan	The Certification Plan is a deliverable that outlines the Solution Vendor's scope of responsibilities related to CMS certification and how they will interact with all stakeholders. It also details tools, reports, evidence collection processes that will be used throughout the project.	Validation that: 1. The Solution Vendor has demonstrated a plan to support certification activities as required throughout the project lifecycle, including producing KPI reports as required for CMS during the O&M phase.	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Design	Final Detailed Design Review	8. Test Management Plan	Contains the testing strategy for different types of testing, including Unit Testing, functional testing, regression testing, integration testing, user acceptance testing, performance testing, manual and automated and/or scripted testing, disaster recovery and end-to-end integration testing. Contains: 1. Testing schedule 2. Testing personnel 3. Training 4. Testing meetings 5. TennCare involvement 6. Collaboration with other vendors 7. Test cases, scripts and scenarios 8. Test data 9. Test environments 10. Tools 11. Test tracking and results 12. Defect management 13. Re-testing and regression testing 14. Test reporting and metrics.	Validation that: 1. The deliverable includes acceptable plans and specifications, according to the Test Management Standard and the deliverable definition.	Type C
Design Implementation	Final Detailed Design Review Operational Readiness Review	9. Functional Design Document	Contains the detailed specifications that outlines the features and behavior of the solution. Will contain detailed process flows and business rules, and may include screen mockups, wireframes, or report mockups. It will contain a description of each solution component, including basic functions and the business areas supported. May contain the following artifacts defined in the EA Modeling Standard: User Roles, System Process Model, Business Rules, State Transition Diagram.	Validation that: 1. The functional requirements in the RTM are addressed by the detailed solution design.	Type C
Design Implementation	Final Detailed Design Review Operational Readiness Review	10. Technical Design Document	Contains the detailed specifications that will communicate the technical details required to develop the solution. It contains: 1. Technical architecture 2. Static code analysis (if applicable) 3. Code quality analysis (if applicable) 4. Enterprise system diagrams, including all components, identifying all logic flow, data flow, systems functions, and their associated data storage 5. A bi-directional traceability to requirements and test plan May contain the Solution Architecture Model as defined in the EA Modeling Standard. Aligned to the TennCare Application Landscape and Inventory. See also the models in the Functional Design Document and the Infrastructure Plan.	Validation that: 1. The solution requirements show clear linkages to design components and are supported by defined acceptance test criteria 2. The design has demonstrated compliance with State and Federal accessibility requirements including Section 508 standards 3. Any identified design gaps have been documented and addressed as managed in the Risk Register / Exception Plan	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				4. The design supports and aligns with the State's solution release strategy 5. Completed assessment of all security controls related to requirements 6. The design addresses data conversion issues at the appropriate level.	
Design	Final Detailed Design Review	11. Interface Control Design Document	A comprehensive report of a system interface. The Interface Control Design Document describes flow of data between systems. It describes the concept of operations, defines the governance of the data exchange, and identifies the communication paths of the expected data flow. Aligned with the TennCare Interface Landscape and Inventory.	Validation that the Interface Control Design Document defines: 1. The interface scope 2. The interface requirements 3. The interface performance requirements 4. The message formats or file layouts 5. The field/element level definitions for the data packets 6. The communication protocols for the interface 7. The security requirements for the interface	Type C
Design	Final Detailed Design Review	12. Data Sharing Agreement	The data sharing agreement is a formal contract between two or more parties clearly outlining what data is required, how the data will be provided through system integration and the purpose and use of the data.	Validation that: 1. The deliverable is in accordance with the contract defined in the deliverable definition and with the deliverable expectation document.	Type C
Design	Final Detailed Design Review	13. Infrastructure Plan	The detailed design of how the solution will be implemented either on-premises or in the cloud. Specifies: 1. The technologies, sizes and connections of the hosting platform, servers and network infrastructure (if applicable) 2. A Capacity and Performance Plan showing how those technologies will achieve the volume and performance requirements. 3. The deployment model, network topology, and System Architecture Design Document. Includes the STS Solution Design Package for on-premises hosting, or a Cloud Design Package for cloud hosting. May contain the following artifacts defined in the EA Modeling Standard: Deployment Model, Network Topology.	Validation that: 1. The deliverable is in accordance with the contract defined in the deliverable definition and with the deliverable expectation document.	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Design Implementation Operations & Maintenance	Final Detailed Design Review Operational Readiness Review Post-Implementation Review	14. Master Data Management Plan	The Master Data Management Plan will include approach, strategy, architecture, methodology, process, tools, resourcing, quality and contingency aspects. The MDM Plan shall make data available to integrate with TennCare's project management tools and support ongoing alignment with TennCare Data Policies and Standards and maintain compliance as these standards evolve.	Validation that: 1. The deliverable is in accordance with the contract defined in the deliverable definition and with the deliverable expectation document.	Type C
Design	Final Detailed Design Review	15. Data Conversion/ Management Plan	Will contain data conversion logical/technical architecture, including mapping documents with associated business rules, strategy to profile, clean, and consolidate data. Contains the Data Transformation Mapping as defined in the EA Modeling Standard.	Validation that: 1. The plan shall describe the assumptions/constraints/risks related to the data conversion 2. The plan shall describe the strategy related to the data conversion which includes the conversion scope, conversions approach, roles and responsibilities (RACI), Conversion Schedule, Data Quality Controls 3. The plan shall describe the process for data conversion preparation which includes prerequisites, backup strategy and restore process 4. The plan shall describe data conversion specifications which includes data dictionaries and data mappings.	Type B
Design	Final Detailed Design Review	16. Database Design	A record layout of each data store with data element definitions. Includes the logical and physical database design, and data dictionary. May contain the following artifacts defined in the EA Modeling Standard: Logical Data Model, Physical Data Model, Report Specification. Aligned with the TennCare Data Landscape and Inventory.	Validation that: 1. The deliverable aligns to the conceptual data model described in the Concept of Operations 2. The design is in alignment with TennCare modeling standards 3. The design is in alignment with TennCare Data Policies and Standards.	Type C
Design	Final Detailed Design Review	17. Project Change Management Plan	Identification of a change control board along with primary and backup members assigned. Contains: 1. Categorization of change types (e.g., standard, emergency, etc.) 2. Processes for requesting, tracking, and performing impact analyses for each change request 3. Processes for deciding whether to approve changes and for verifying that changes were made correctly.	Validation that: 1. The plan is developed in accordance with the TennCare Information Systems Lifecycle 2. The plan is developed in accordance with the Project Change Management Standard	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				3. Project Change Management Plan aligns with and is approved by TennCare's Enterprise Change Management Processes 4. Change Management Plan DED has been created and approved by TennCare 5. Simultaneous approval of the Configuration and Deployment Management Plan, Contract Management Plan, and Organizational Change Management (OCM) Plan. 6. Simultaneous approval of the Project Change Request Template.	
Development	Validation Readiness Review	18. Training Plan	A detailed approach to planning for training delivery and the development of training environments and materials in collaboration with TennCare Organizational Change Management and Training team and their partners in accordance with TennCare's training strategy.	Validation that: The Training Plan should provide the detailed approach, in accordance with the State's training strategy at that point in time, to the following: 1. Collaboration with TennCare and its partners 2. Descriptions of training solutions for both highly technical and non-technical users across the Enterprise 3. The inclusion and development of a training environment 4. Necessary hardware and/or software installations 5. Training curricula 6. The approach to and delivery of a train the trainer program 7. Procedures for maintaining documentation for each functional area, screen layouts, report layouts, and other output definitions, including examples and content definitions 8. The creation of training materials and job aids, including but not limited to- user manuals, business rules, and all other documentation appropriate to the platform, operating systems, and programming languages	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				9. Knowledge transfer programs for highly technical and non-technical Users across the Enterprise.	
Development	Validation Readiness Review	19. Unit Test Report	Unit Test Cases, Scripts, Data, Results & Mitigation Plan Declares that the solution vendor has completed the Unit Testing stage for a module. It indicates: 1. What module version was tested, with what data on what environment 2. The percentage of test cases passed, failed, and not completed 3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect.	Validation that: 1. The Unit and Connectivity test cases are approved (as an appropriate and complete set) 2. 100% of approved Unit and Connectivity test cases are tested (completed) 3. Threshold % of Unit and Connectivity test cases are successful (passed) (the threshold percentage is to be defined in the RFP, Contract, or approved Module Test Plan) 4. All defects have been logged in the defect management tool with a severity level 5. Defects are fixed where feasible 6. All unresolved defects have a mitigation plan approved by TennCare.	Type B
Development	Validation Readiness Review	20. Implementation Plan	The detailed steps that will be required to implement the solution into production from the development cycle, including processes, resources, roles and responsibilities, support during deployment, confirmation that data is available and accurate, and the transition to the operating organization. The Implementation Plan must include a bill of materials for what will be implemented, describing what the solution contains e.g., software components, technology components and tools, backup technologies and server/storage, etc.	Validation that: 1. The Implementation Plan addresses the required activities and are sequenced accordingly, with defined roles and responsibilities. 2. The plan shall describe the assumptions/constraints/risks related to the implementation approach 3. The plan shall describe the phased approach focusing on costs and longer-term goal for the project across all work streams 4. The plan shall include the project scope, approach and resource plan 5. The plan shall describe a bottom-up approach to calculate the development effort and team structure that derives from the resource plan.	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Development	Validation Readiness Review	21. Business Continuity/Disaster Recovery Plan	The detailed processes, techniques and activities that are required to continue routine business operations in the event of a disaster. This plan defines: 1. The processes and procedures for business continuation, including: a. key staff b. required equipment 2. Disaster recovery plans for the solution, communications, hardware, and any IT assets (if applicable) 3. Analysis of potential threats 4. Areas of responsibility 5. Emergency contact information 5. Recovery Teams 6. Data and Solution Recovery 7. Communications Strategy 8. Essential Services backup 9. Recovery to pre-disaster state	Validation that: 1. The BC/DR contain detailed processes and activities required to operate the business in the event of a disaster 2. The detailed processes and steps for recovering solutions to a pre-disaster state.	Type C
Development	Validation Readiness Review	22. Incident Management Plan	Defines: 1. What constitutes an incident, incident classifications, severity levels, and target times for resolution 2. Processes for reporting, logging, managing, and tracking incidents to resolution and closure 3. Process for communicating with affected stakeholders 4. Identification of an incident manager 5. Determining criteria for creating Problems from Incidents 6. Event Management Plan 7. Problem Management Plan 8. System Incident and Corrective Maintenance Reports 9. Contains vendor's general contact information for indecent notification and specific individual(s) with roles to contact in the event of a security or privacy incident. 10. Describes how the vendor will communicate and notify TennCare Security and Privacy regarding incidents from incident inception through resolution. 11. Corresponds to the Incident Response Plan that meets federal, State of Tennessee, and TennCare contractual requirements for the Data Types contained. (CMS template available)	Validation that: 1. The Incident Management Plan contains detailed definitions and processes for the identification, categorization, mitigation, and reporting of encountered incidents. 2. Additionally, the plan contains comprehensive details related to event and problem management.	Type B
Development	Validation Readiness Review	23. Security Management Plan	The Security Management Plan is a planning phase Security deliverable that describes how a project team or vendor plans to staff and manage Security activities for the project	Validation that: 1. Information in the Security Management Plan Template meets or	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			Implementation and O&M. This is used at the very beginning of the project to ensure that proper resources, functions, and teams are being properly aligned specific to supporting the successful security and privacy of the project. This document should include at minimum the below sections. A more detailed Template is located on the TennCare Security Intranet site (template in development). 1. Scope 2. Descriptions, Objectives, and Methodology 3. Contracts, Statement of Work, Control Letters 4. Planned Deliverables 5. Staffing Roles and Responsibilities 6. Contacts 7. Training 8. Incident Response Coordination 9. Current or Planned Certifications 10. Key Milestones 11. Subcontractors.	exceeds the required fields identified in the template.	
Test	Implementation Readiness Review	24. System Integration Test (SIT) Report	Contains: 1. Test Cases 2. Test Data 3. Test Scripts 4. Test Reports 5. Test Summary Report 6. Defects & Mitigation.	Validation that: 1. The System Integration Testing (SIT) test cases are approved (as an appropriate and complete set) 2. 100% of approved SIT test cases are tested (completed) 3. All critical and blocking defects (from SIT or previous stages) have been resolved 4. All unresolved defects have a mitigation plan approved by TennCare.	Type B
Test	Implementation Readiness Review	25. User Acceptance Test (UAT) Report	Contains: 1. Acceptance testing report for each user story/use case 2. Formal Acceptance Testing Report 3. System Readiness Certification for User Acceptance Test (UAT) 4. Test Reports 5. Test Summary Report 6. Unit, System, and Integration Testing Test Results 7. Automated Code Review Results.	Validation that: 1. The UAT test cases are approved (as an appropriate and complete set) 2. 100% of approved UAT test cases are tested (completed) 3. All critical and blocking defects (from UAT or previous stages) have been resolved 4. All unresolved defects have a mitigation plan approved by TennCare	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				5. The TennCare UAT testing team accepts the solution module.	
Test Operations & Maintenance	Implementation Readiness Review Post-Implementation Review	26. System Security Plan (SSP)	Utilizing the TennCare System Security Plan template (based on the CMS MARS-E standard), documents the strategies and state policies for handling privacy, security, and HIPPA compliance. Contains: 1. Completion of Part A – System Identification a. Executive summary providing a short, high-level description appropriate for achieving an executive level understanding of what the system is, what sensitive data it processes, and what key protections have been applied; b. System identification providing an overall description of the business process(es) associated with the IT system and an overall description of the IT system environment supporting the business function. 2. Completion of Part B – Security Controls a. Implementation descriptions of the integrated security controls detailing how the system addresses the requirements and standards 3. Completion of Part C – Privacy Controls a. Implementation descriptions of the integrated privacy controls detailing how the system addresses the requirements and standards b. Each SSP must include a response for three entities at a minimum: TennCare, STS, and the system-specific implementation responses. 4. Completion of Part D – SSP Attachments a. Equipment listing consistent with CM-8 (Configuration Management as per NIST 800-53) that supports the system/application b. Software listing consistent with (Configuration Management as per NIST 800-53) that supports the system/application c. Detailed configuration settings consistent with CM-2 (Configuration Management as per NIST 800-53) and CM-6 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations d. SSP acronyms and abbreviations used in the SSP that are not defined in MARS-E e. SSP glossary containing terms used in the SSP that are not defined in MARS-E 5. Additional Artifacts as detailed in Table B-1. MARS-E Security and Privacy Agreements and Compliance Artifacts which includes MARS-E documentation of detailed system security posture and control implementation descriptions.	Validation that: 1. The submitted schedule is in alignment with and addresses the requirements defined in the deliverable expectations document and the deliverable definition.	Type D

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			May contain the Security Boundary Model as defined in the EA Modeling Standard.		
Test Operations & Maintenance	Implementation Readiness Review Post-Implementation Review	27. Privacy Impact Assessment	Utilizes CMS template for overall privacy analysis of the system. The PIA applies to a single system, and the analysis is completed based upon the privacy within the security boundary of the system being implemented.	Validation that: 1. The PIA only documents a single system contained within a single security boundary. The PIA may NOT contain multiple system across security boundaries. 2. The CMS Privacy Impact Assessment (PIA) Template that has all response fields completed with accurate and comprehensive responses.	Type C
Test Operations & Maintenance	Implementation Readiness Review Post-Implementation Review	28. Information Security Risk Assessment	Utilizes CMS template report for Risks as a result of an identified Weakness [Plan of Action & Milestone (POA&M)] or Risk Acceptance from baseline controls and standards in MARS-E. As part of an iterative document development process, the documents note business and technical risks starting near the completion of the design process and continues until the system is ready to be placed into production. The first final submission is part of the ATO package and updated annually or in the event of a significant system change thereafter, whichever comes first.	Validation that: 1. The CMS Information Security Risk Assessment (ISRA) Procedure have accurately been followed and that has all response fields completed with accurate and comprehensive responses. 2. The ISRA shall document security, privacy and business risks related to the operation and use of the system. 3. Describes the implementation of effective and timely controls and mitigation measures to minimize risk exposures including plans for addressing security and privacy risks, documents the risks associated with the system, describes processes to measure and monitor risks associated with the system.	Type C
Implementation	Operational Readiness Review	29. Operational Readiness Test (ORT) Report	Each Test Report declares that the solution vendor has completed a stage of testing of a module. It indicates: 1. What module version was tested, with what data on what environment 2. The percentage of test cases passed, failed, and not completed 3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect.	Validation that: 1. The Operational Readiness Test (ORT) test cases are approved (as an appropriate and complete set) 2. 100% of approved ORT test cases are test (completed) 3. All critical and blocking defects (from ORT or previous stages) have been resolved	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				4. All unresolved defects have a mitigation plan approved by TennCare 5. The TennCare IS testing team accepts the solution module.	
Implementation	Operational Readiness Review	30. Beta Test Report	Each Test Report declares that the solution vendor has completed a stage of testing of a module. It indicates: 1. What module version was tested, with what data on what environment 2. The percentage of test cases passed, failed, and not completed 3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect.	Validation that: 1. Beta or Pilot testing has been completed as planned 2. All critical and blocking defects have been resolved 3. All unresolved defects have a mitigation plan approved by TennCare 4. The TennCare Business and IS testing team accepts the solution module.	Type B
Implementation	Operational Readiness Review	31. Turnover Plan	Documentation that describes how a solution is transitioned to another vendor or to TennCare for continued operation. The plan will include: 1. Data Turnover tasks; 2. Custom Interface Turnover tasks; 3. Reusable code, configurations, and Turnover tasks; 4. Documentation regarding products (with versions), files, interfaces, and work flows not considered to be part of the COTS proprietary documentation tasks; and 5. A timeline with milestones for the Turnover to include planning, execution, and implementation approval.	Validation that: 1. The plan contains a list of all tasks, timeline and milestones required to perform the Turnover 2. The plan contains complete documentation of the solution as described in the deliverable definition.	Type C
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	32. Operations & Maintenance Run Book	Product documentation that describes how to operate the solution. Contains: 1. Operations manuals 2. Standard operating procedures (SOP Manual) 3. User guides 4. List of all error codes and explanations by component 5. Infrastructure Services Deployment Report 6. Infrastructure, System Source Code, and Documentation 7. Manuals and Training Materials 8. Operations & Support procedures 9. System Configuration Document 10. System Operations Documentation 11. Training Artifacts	Validation that: 1. Evidence that Transformed Medicaid Statistical Information Systems (T-MSIS) data requirements have been met for timeliness and data quality (if required) 2. The solution build is code-complete and there are no outstanding critical or high development defects. 3. There are no missing features or media elements, and the initial release of the solution build is available and has completed thorough development testing activities.	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			12. Training Plan 13. Updated Infrastructure System Source Code and Documentation 14. A substantive and representative set of all reports and information retrieval screens (electronic format preferred) 15. A list of information retrieval functions and reports for each business area (including a list that identifies the distribution of the reports and who can access the information retrieval displays) 16. Plan for rolling out the new or updated module/system to the users 17. Implementation and Deployment Plan 18. Performance, Availability and Capacity Plan 19. Release and Deployment Plan 20. Service Transition Plan 21. System Maintenance, Support, and System Transition Plan 22. Cutover Plan.		
Implementation	Operational Readiness Review	33. Authority to Operate (ATO)	Formal signoff by TennCare Business/System Owner acknowledging they have performed their diligence for Privacy, Security, and Operations and authorizing production to go-live.	Validation that: 1. All initial security and privacy documentation and test are completed and approved.	Type A
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	34. Security Assessment Plan	This Security and Privacy Assessment Plan (SAP) documents all testing to validate the security and privacy controls for a system. The Security Assessment Plan must be delivered to CMS a minimum of sixty (60) days prior to the kickoff of the Third-Party Independent Assessment. The plan is completed by the third-party assessor for the benefit of TennCare and federal regulators. Following the Framework for Independent Assessment of Security and Privacy Controls, the assessment plan documents how the assessor will evaluate: 1. System compliance with security & privacy controls in the SSP 2. Underlying infrastructure's security posture 3. The system and data security and privacy posture 4. Proper security configuration associated with the database or file structure storing the data 5. Systems technical, managerial, and organizational adherence to the organization's security and privacy program, policies, and guidance.	Validation that: 1. The project has an acceptable risk vs. return, addresses high-priority business needs and mandate, and has the most preferable alternative to meeting the business need. 2. Identifies all high-level risk and that the Business Owner has accepted preliminary mitigation or contingency plans.	Type B
Implementation Operations & Maintenance	Operational Readiness Review	35. Third-Party Security and Privacy Assessment	The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy	Validation that: 1. The full assessment report, associated report, and findings are	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
	Post-Implementation Review		requirements of the application or system. The SCA also identifies areas of risk that require the State's attention and remediation. Independent review as defined by CMS of control effectiveness using SSP Control Set and NIST 800-53A review methods with required guidance from CMS MARSE template and guidance on conducting "Independent Third-Party Security and Privacy Audit Guidelines for Medicaid Enterprise System (MES) Outcome Based Certification (OBC). The third-party security and privacy assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness. At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to TennCare's Business Owner, who is then responsible for providing the report to CMS. The SAR content includes the following information: 1. System Overview 2. Executive Summary Report 3. Detailed Findings Report 4. Scan Results: i. Infrastructure Scan ii. Database Scan iii. Web Application Scan 5. Penetration Test Report 6. Penetration Test and Scan Results Summary.	provided to TennCare security and privacy teams. 2. The security and privacy teams agree that the assessment tested the right items, performed a thorough scan of all these items, and that the report accurately reflects this. 3. Any minimal security/privacy risks that were found are being remediated and the remediation plan is being reported on to TennCare.	
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	36. Plan of Actions and Milestones	Plans of Actions and Milestones: At the latest is created and reported upon completion of the Security Assessment Report detailing remediation of any "planned" control actions or assessment findings needing remediation. These findings are logged, tracked and updated in the TennCare electronic Governance Risk and Compliance system on a monthly basis by the vendor. These may be temporarily tracked using the CMS provided POA&M spreadsheet with the approval of the TennCare Chief Security Officer.	Validation that: 1. Risk and findings are logged in the CMS POA&M format within the TennCare Governance Risk and Compliance (GRC) system. 2. Vendor completes monthly updates to all POA&Ms after initial submission 3. Vendor attends monthly POA&M meetings with TennCare Security.	Type B
Implementation	Operational Readiness Review	37. Enterprise Intake Form	Outcomes Based Certification (OBC) required document provided by CMS that details the Enterprise level requirements that a new module/system should demonstrate and meet.	Validation that: 1. Each criteria within the intake form has a response and the TennCare	Type A

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Operations & Maintenance	Post-Implementation Review		Includes a variety of requirements and expected documentation. Provides CMS information on how TennCare meets the criteria for the enterprise but also how the module being certified will contribute to the enterprise criterion. This form is updated after implementation certification, again for operations certification to show how the module being certified is contributing to the enterprise criterion and again with any updates after operation certification that are requested by CMS.	owners have signed-off on each response.	
Implementation	Operational Readiness Review	38. Module Intake Form	OBC required document provided by CMS that details the module specific requirements that a new module/system should demonstrate and meet. Includes a variety of requirements, expected documentation, and test objectives	Validation that: 1. Each criteria within the intake form has a response and the TennCare owners have signed-off on each response	Type A
Operations & Maintenance	Post-Implementation review	39. Contingency Plan	Standard NIST based methods for documenting Continuity and Disaster Planning as defined in SP 800-34.	Validation that: 1. Information contained in the plan meets or exceeds the standards in NIST SP 800-34 2. The Contingency Plan meets or exceeds the requirements in the current version of MARS-E Contingency Planning (CP) family of security controls, control enhancements, and implementation standards as defined in the System Security Plan template as applicable. 3. The Contingency Plan meets or exceeds the requirements in the current version of MARS-E related control requirements for the Contingency Planning (CP). These are listed in the "Related Control Requirement(s) section of the System Security Plan Template.	Type C
Operations & Maintenance	Post-Implementation Review	40. Official Certification Request Letter	Required for Outcomes Based Certification with CMS and produced six months after solution go-live. Contains: 1. The date the system became fully operational 2. A copy of TennCare's letter to the Solution Vendor accepting the system/modules(s) 3. A copy of the official acceptance letter from TennCare to the Solution Vendor 4. A proposed timeframe for the review 5. A declaration that TennCare's DE Component meets all of the requirements of law and regulation:	Validation that: 1. TennCare agrees that TennCare is ready for certification. All evidence/reports have been signed-off on, uploaded to SharePoint, and/or sent to CMS.	Type A

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			i. Meets the requirements of 42 CFR 433.117 for all periods for which the 75-percent FFP is being claimed ii. Issues Explanation of Benefits (EOBs) on a regular basis for all periods for which 75-percent FFP is being claimed, in accordance with the provisions of Section 10 of P.L. 95142, which amends section 1903(a)(3) of the Social Security Act iii. Is ready for CMS certification, based on TennCare's evaluation using the checklists in the Toolkit iv. Generates up-to-date and accurate T-MSIS (Transformed Medicaid Statistical Information Systems) data if required v. Routinely generates backups containing up-to-date and accurate T-MSIS data vi. Exercises appropriate privacy and security controls over the system in accordance with 45 CFR Part 164, P.L. 104-191, HIPAA of 1996, and 1902(a)(7) of the Social Security Act as further interpreted in regulations at 42 CFR 431.300 to 307.		
Operations & Maintenance	Post-Implementation Review	41. KPI Report	Module-Specific and Enterprise Key Performance Indicators (KPI) that demonstrate the system is meeting business objectives. This includes several KPI calculations that the Solution Vendors are expected to run and produce on an agreed-upon basis continuously after go-live. Module solution vendors would produce module-level KPI reports, and the IS Solution Vendor would produce enterprise or IS-level KPI reports.	Validation that: 1. Each KPI calculation can be completed with appropriate results generated by the DDI vendor. 2. TennCare owners have signed off on each KPI result.	Type A
Retire	Disposition Review	42. System Disposition Plan / Report	Documents how the various components of an automated system (software, data, hardware, communications, and documentation) are to be handled at the completion of operations to ensure proper disposition of all the system components and to avoid disruption of the individuals and/or other systems impacted by the disposition.	Validation that: 1. The solution/system has been successfully disposed in accordance with the System Disposition Plan 2. TennCare has approved the System Disposition Report and verified that the appropriate activities have taken place: a. The system is properly shutdown b. Project archives are located in the correct place and on the correct medium c. System security and data procedures were followed correctly to ensure the protection of private or sensitive data and that there is no user access to the system/application/solution d. Any continued use of system or application components are done in	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				accordance within State security requirements and are fully documented in the System Disposition Report e. Final phase-end review has been conducted after the system retirement to ascertain if the system and data have been completely and appropriately disposed of f. Security objectives, including secure data and system transfer, sanitization and disposal of media has been accomplished g. Project Archives that preserve vital information, including both documentation of project execution and the data from the production system has been appropriately preserved.	

B. TERM OF CONTRACT:

B.1. This Contract shall be effective on September 1, 2022 ("Effective Date") and extend for a period eighty-four (84) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to three (3) one-year renewal options under the same terms and conditions for a period not to exceed thirty-six (36) months by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of one hundred twenty (120) months.

C. PAYMENT TERMS AND CONDITIONS:

C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed Fifty-Four Million Two Hundred Fifty Thousand One Hundred Thirty-Eight Dollars and Twenty-Seven Cents ($54,250,138.27) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. Compensation Firm. The payment methodology in Section C.3. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor. The Contractor shall ensure that:

a) Data transfer tools, capacity, and cost as required by A.9.1.13 shall be included in the Maximum Liability and shall not result in additional cost to TennCare during the Contract.

b) Data storage tools, capacity, and cost as required by A.9.1.14 shall be included in the Maximum Liability and shall not result in additional cost to TennCare during the Contract.

c) Archiving tools, capacity, and cost as required by A.9.1.15 shall be included in the Maximum Liability and shall not result in additional cost to TennCare during the Contract.

d) Data restore tools, capacity, and cost as required by A.9.1.16 shall be included in the Maximum Liability and shall not result in additional cost to TennCare during the Contract.

e) Cloud services as required by A.9.1.17 shall be included in the Maximum Liability and shall not result in additional cost to State of Tennessee or TennCare during the Contract.

f) An increase in required capacity within the MMP scope as required by A.9.4.1 shall be included in the Maximum Liability and shall not result in an increased cost to TennCare.

g) All costs associated with the facility as required by A.12.5 are the responsibility of the Contractor for the entire Contract period. Such costs shall be included in the Maximum Liability of the Contract and shall not be billed separately or result in an increased cost to TennCare; and

h) All goods or Services, as applicable to the DE Component, to satisfy the requirements in Sections A.3 through A.12 shall be included in the Maximum Liability and shall not result in additional cost to TennCare.

C.3. Payment Methodology. The Contractor shall be compensated based on the payment methodology for goods or services in Attachment G, Cost Proposal and as authorized by the State in a total amount as set forth in Section C.1.

a) The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

1. The design, development, testing, and implementation phases include all Deliverables and other activities required in the TennCare Solution Implementation Lifecycle. The standard method for Payment under this Contract to Contractor shall be made according to Section C of this Contract upon TennCare certification of a successful

unconditional pass of the Gate Review (as described in this Section) and TennCare approval of all Deliverables associated with the Gate Review. Each of the Gate Reviews constitutes a subset of Deliverables that the Contractor must deliver during the implementation of the DE Component.

2. Data Source Payment

    a. Each Data Source integrated during DDI, once approved by TennCare, will be a Deliverable during DDI. Upon delivery and TennCare Acceptance of each unique Data Source within the allocated data source type and number in the TennCare Data Sources Service Type – Definitions and Scoring, the Contractor will be paid the applicable payment designated by DE Component and Complexity Type in Attachment G, Column E, Cost Proposal, in accordance with this Section.

    b. Each Data Source integrated during O&M, once approved by TennCare, will be a Deliverable during O&M. Upon delivery and TennCare Acceptance of each unique Data Source within the allocated data source type and number in the TennCare Data Sources Service Type – Definitions and Scoring, the Contractor will be paid the applicable payment designated by DE Component and Complexity Type in Attachment G, Column E, Cost Proposal, in accordance with this Section.

    c. For each unique Data Source integrated after the allocated Data Source type and number included in the TennCare Data Sources Service Type – Definitions and Scoring has been exhausted, integration will be authorized and funded through the Change Order process in accordance with A.12.7. Upon delivery and TennCare acceptance of each Data Source, the Contractor will be paid no more than the applicable payment designated by DE Component and Complexity Type in Attachment G, Column E, Cost Proposal, in accordance with this Section.

3. In the event that a Change Order necessitates changes to a Deliverable approved in a previous Gate Review, TennCare shall consider the revised Deliverable to be a required Deliverable with the next Gate Review or subject to TennCare approval prior to enhancement release.

4. Following the unconditional pass of the Post Implementation Review Gate, the Contractor shall begin monthly O&M reporting, and the Contractor shall invoice the monthly O&M cost as described in this Section.

5. In exceptional circumstances and solely on its own initiative and discretion, TennCare may alter the Payment and withhold structure, set forth in C.3(a)(1). Such alterations shall be governed by the Control Memorandum process and may include:

    a. TennCare may pay Contractor an amount in excess of the amount due at the time of a successful Gate Review if the Contractor has completed a functionality or functionalities scheduled to be included in a subsequent Gate Review. Any such excess amount will be deducted or withheld from the amount due to the Contractor upon the successful subsequent Gate Review that was originally intended to include that functionality or functionalities.

    b. TennCare may alter the amount of the withhold for any particular Gate Review Payment as set forth in this Section.

6. In no event shall any alteration set forth above:

    a. increase the total amount due to the Contractor from TennCare under this Contract;

    b. result in a delay or reduction of any Payment to the Contractor, except to the extent that funds have previously been paid to the Contractor as a result of an alteration; or

c. be used to compensate the Contractor for any work which has not been completed at the time that the alteration of the Payment or withhold structure is made.

7. The alteration to the Payment and withhold structure shall be deemed to be made at the time that TennCare notifies the Contractor in writing.

8. The Contractor agrees that the determination by TennCare that exceptional circumstance(s) exist (or do not exist) and the determination of the type, amount and timing of any alteration if any, is the sole prerogative of TennCare and is not subject to review.

b) The Contractor shall be compensated based upon the following payment methodology as detailed in Attachment G, Cost Proposal:

Goods or Services Description	Amount (per compensable increment)
DDI Phase: Gate Review 1 – Project Startup Review Data Quality/ETL Pipeline Component	$1,515,534.79
DDI Phase: Gate Review 4 – Requirement Review Data Quality/ETL Pipeline Component	$3,788,836.98
DDI Phase: Gate Review 7 - Implementation Readiness Review Data Quality/ETL Pipeline Component	$3,031,069.58
DDI Phase: Acceptance Letter Data Quality/ETL Pipeline Component	$5,304,371.77
DDI Phase: Completion of Warranty Period Data Quality/ETL Pipeline Component	$1,515,534.79
Operation & Maintenance Phase: Monthly Services— Year 1 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Year 2 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Year 3 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Year 4 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Year 5 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Optional Year 1 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Optional Year 2 Data Quality/ETL Pipeline Component	$1,718,565.96
Operation & Maintenance Phase: Monthly Services— Optional Year 3 Data Quality/ETL Pipeline Component	$1,718,565.96
Data Source Integration - Data Quality/ETL Pipeline Component	$12,827,000.00

c) The Contractor shall be compensated for Special Project Change Orders and Enhancement Change Orders requested and performed pursuant to Contract Section A.12.7 without a formal amendment of this Contract based upon the allocated amount in the Special Projects and Enhancement funds detailed in Contract Attachment G, Cost

Proposal, Schedule A, based upon rates provided in Schedules C, and/or E, PROVIDED THAT:

1) Compensation to the Contractor for Special Project Change Orders shall not exceed fifteen 15% the sum of the Total DDI and O&M Costs above (which is the total cost of the DDI and the O&M Phase).
   a. Special Project Change Orders shall be paid upon the successful unconditional pass of the associated Gate Review and TennCare Acceptance of all associated Deliverables.
   b. All Special Projects shall be associated with a Gate Review as determined by TennCare and not paid until approved as part of the Gate Review process.
2) Compensation to the Contractor for Enhancement Change Orders shall not exceed the cost associated with fifteen (15%) of the sum of the Total DDI and O&M Costs above (which is the total cost of DDI and the O&M Phase).
   a. Enhancement Change Orders shall be paid upon successful release of the enhancement functionality as determined by TennCare, in its sole discretion
3) INTENTIONALLY OMITTED.
4) If, at any point during the Term, the State determines that the cost of necessary Special Projects and Enhancements work would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	Amount (per compensable increment)
Special Project Change Order Requests	**$6,259,631.34** **(15% of the Total DDI & O&M Costs; Attachment G, Schedule A)**
Enhancement Change Order Request	**$6,259,631.34** **(15% of the Total DDI & O&M Costs; Attachment G, Schedule A)**

C.4. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3, above. All invoices submitted for any and all services rendered by Contractor's staff and subcontractors (resource reporting), the invoice shall, at a minimum, include the name of each individual, the individual's role classification, the number of hours worked during the period, the applicable Payment Rate, the total compensation requested for the individual, and the total amount due the Contractor for the period invoices. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

NAME

Division of TennCare
310 Great Circle Road
Nashville, TN 37243

a) Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):
   1) Invoice number (assigned by the Contractor);
   2) Invoice date;
   3) Contract number (assigned by the State);

4) Customer account name: Department of Finance and Administration, Division of TennCare;

5) Customer account number (assigned by the Contractor to the above-referenced Customer);

6) Contractor name;

7) Contractor Tennessee Edison registration ID number;

8) Contractor contact for invoice questions (name, phone, or email);

9) Contractor remittance address;

10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;

11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;

12) Applicable payment methodology (as stipulated in Section C.3) of each good or service invoiced;

13) Amount due for each compensable unit of good or service; and

14) Total amount due for the invoice period.

b) Contractor's invoices shall:

1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;

2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;

3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and

4) Include shipping or delivery charges only as authorized in this Contract.

c) The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.

a) The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by Automated Clearing House; and

b) The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Deputy Commissioner
Department of Finance and Administration Division of TennCare
310 Great Circle Road
Nashville, TN 37243
Telephone # (615) 507-6444

The Contractor:

Deborah Hall, Account Executive
IBM
1 New Orchard Road
Armonk, NY 10504
debbie.hall@us.ibm.com
Telephone # (470) 349-1938

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

D.3. All information or data that is necessary for one or more deliverables set forth in this Contract shall be transmitted between TennCare and Contractor via the data transfer method specified in advance by TennCare. This may include, but shall not be limited to, transfer through TennCare's SFTP system. Failure by the Contractor to transmit information or data that is necessary for a deliverable in the manner specified by TennCare, may, at the option of TennCare, result in Liquidated Damages as set forth in Contract Attachment B. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.

D.4. Subject to Funds Availability**.** The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the

State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination**.** The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination. In addition, the Contractor shall comply with the provisions of Contract Section E.35 (Nondiscrimination Compliance Requirements) and this Section D.9 shall not be deemed to limit or abridge any requirement set forth in Section E.35.

D.10. Prohibition of Illegal Immigrants**.** The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a) The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Contract

Attachment E, Attestation Re: Personnel Used in Contract Performance, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b) Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c) The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d) The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

e) For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

D.11. Records**.** The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of ten (10) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.

D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.

D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

D.16. Patient Protection and Affordable Care Act**.** The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs

to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.

D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims, including Contractor's obligations under Section E.20 (Personally Identifiable Information) and Section E.28(g) (Social Security Administration (SSA) Required Provisions for Data Security, arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1 and as may be amended. Except as set forth below in this Section, in no event will the Contractor be liable to the State or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for Liquidated Damages set forth in Attachment B, Service Level Agreements and Liquidated Damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death. For clarity, except as otherwise expressly set forth in this Section, Contractor's indemnification obligations and other remedies available under this Contract are subject to the limitations on liability set forth in this Section.

D.19. Hold Harmless**.** The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of wrongful acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys' fees, court costs, expert witness fees, and other litigation expenses for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.20. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

a) Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

b) Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the

Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

c) The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

d) The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

D.21. Tennessee Consolidated Retirement System**.** Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, et seq., the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, et seq., accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22. Tennessee Department of Revenue Registration**.** The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.23. Debarment and Suspension**.** The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

a) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

b) have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

c) are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

d) have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

D.24. Force Majeure**.** "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-

performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees for the affected obligation until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

D.25. State and Federal Compliance**.** The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.

D.26. Governing Law**.** This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee, without regard to its conflict or choice of law rules. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 – 408.

D.27. Entire Agreement**.** This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

D.28. Severability**.** If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.

D.29. Headings**.** Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

D.30. Incorporation of Additional Documents**.** Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

a) any amendment to this Contract, with the latter in time controlling over any earlier amendments;

b) this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes:

1) Attachment A – Definitions and Abbreviations;

2) Attachment B – Service Level Agreements and Liquidated Damages for DQ/ETL;

3) Attachment C – Procurement Library;

a. TennCare Data Sources Service Type – Definitions and Scoring
b. DE TennCare Solution Implementation Lifecycle RACI and Deliverables
c. TennCare Enterprise Architecture Framework Standard
d. MDM Compendium
e. Data Ecosystem Volumetric Information
f. Application and Interface Integration Inventory
g. TennCare Reporting Reference Guide for Data Ecosystem
h. TennCare Data Conversion Standard
i. TennCare Solution Implementation Lifecycle (SILC) Standard
j. TennCare Test Management Standard
k. TennCare Project Change Management Standard
l. TennCare Project Change Management Standard RACI
m. TennCare Project Management Plan Standard
n. TennCare Preferred Technology Standard
o. TennCare Enterprise Architecture Modeling Standard
p. TennCare Requirements Management Standard
q. TennCare IS Governance Standard
r. TennCare Deliverable Template
s. TennCare IT Service Management Standard
t. TennCare IT Service Management RACI
u. TennCare Data Policies and Standards
v. Industry Standards and Policies
w. TennCare Record Retention Policy
x. TennCare Records Disposition Authorization (RDA) List
y. TennCare System Security Plan (SSP) Template
z. TennCare Enterprise Security Policy
aa. Enterprise Information Security Policies
bb. TennCare Privacy Program Policy and Plan (PRIV-028)
cc. TennCare Privacy, Security and Confidentiality Training Policy (PRIV-013)
dd. TennCare Information Security Program Plan (ISPP)
ee. TennCare Enterprise Security Policy - TennCare Mobile Code Policy (interim)
ff. TennCare Enterprise Security Policy - TennCare Password Complexity Policy (interim)
gg. TennCare Enterprise Security Policy - TennCare Personnel Termination Policy (interim)
hh. TennCare Enterprise Security Policy - IRS-FTI Physical Security (interim)
ii. TennCare Organizational Chart
jj. Data Ecosystem Cloud Cost Template

kk. TennCare MDM Data Sources Service Type – Definitions and Scoring

4) Attachment D – Requirements Traceability Overview and Matrix;

5) Attachment E – Attestation Re: Personnel Use in Contract Performance;

6) Attachment F – Business Associate Agreement;

7) Attachment G – Cost Proposal; and

8) Attachment H – EULA.

c) any clarifications of or addenda to the Contractor's proposal seeking this Contract;

d) the State solicitation, as may be amended, requesting responses in competition for this Contract;

e) any technical specifications provided to proposers during the procurement process to award this Contract; and

f) the Contractor's response seeking this Contract.

D.31. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101, et seq., addressing contracting with persons as defined at Tenn. Code Ann. §12-12-103(5) that engage in investment activities in Iran, shall be a material provision of this Contract. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.

D.32. Insurance. Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to amend or require additional insurance coverage, coverage amounts, and endorsements required under this Contract. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Contract. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) acceptable to the State; (b) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (c) rated A- / VII or better by A.M. Best. Commercial General Liability and Automobile Liability coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State respect to liability arising out of this Contract. Contractor agrees to name the State as an additional insured on the Commercial General Liability and Automobile Liability policies. Commercial General Liability and Automobile Liability policies must contain an endorsement for a waiver of subrogation in favor of the State. Any deductible or self insured retention ("SIR") over fifty thousand dollars ($50,000) must be approved by the State. The deductible or SIR and any premiums are the Contractor's sole responsibility. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Contract is for two million dollars ($2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars ($1,000,000) combined with an umbrella policy for an additional one million dollars ($1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area. In the event that an umbrella policy is being provided to achieve any required coverage amounts, the umbrella policy shall be accompanied by an endorsement at least as broad as the Insurance Services Office, Inc. (also known as "ISO") "Noncontributory—Other Insurance Condition" endorsement or shall be written on a policy form that addresses both the primary and noncontributory basis of the umbrella policy if the State is otherwise named as an additional insured.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance Commissioners (NAIC) number and be signed by an authorized representative of the insurer. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI ten (10) business days prior to the Effective Date and again thirty (30) calendar days before renewal or replacement of coverage. Contractor's subcontractors used in the performance of this Contract shall maintain insurance coverages of the types and in the amounts customary for businesses of similar size and in accordance with industry practice.

At any time, the State may require Contractor to provide a valid COI. The Parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Contract. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses. The State reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The insurance obligations under this Contract shall be: the minimum insurance coverage requirements and policy limits shown in this Contract; whichever is greater. No representation is made that the minimum insurance requirements of the Contract are sufficient to cover the obligations of the Contractor arising under this Contract. The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability ("CGL") Insurance

    1) The Contractor shall maintain CGL, which shall be written on an ISO Form CG 00 01 occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises and operations products and completed operations, bodily injury, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

       The Contractor shall maintain single limits not less than one million dollars ($1,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this policy or location of occurrence or the general aggregate limit shall be twice the required occurrence limit.

b. Workers' Compensation and Employer Liability Insurance

    1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:

i. Workers' compensation in an amount not less than one million dollars ($1,000,000) including employer liability of one million dollars ($1,000,000) per accident for bodily injury by accident, one million dollars ($1,000,000) policy limit by disease, and one million dollars ($1,000,000) per employee for bodily injury by disease.

2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:

i. The Contractor employs fewer than five (5) employees;

ii. The Contractor is a sole proprietor;

iii. The Contractor is in the construction business or trades with no employees;

iv. The Contractor is in the coal mining industry with no employees;

v. The Contractor is a state or local government; or

vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).

2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars ($1,000,000) per occurrence or combined single limit.

d. Professional Liability (Errors & Omissions) Liability/Cyber Liability Insurance

1) The Contractor shall maintain technology professional liability (errors & omissions)/cyber liability insurance appropriate to the Contractor's profession in an amount not less than ten million dollars ($10,000,000) per occurrence or claim and ten million dollars ($10,000,000) annual aggregate, covering actual or alleged breach of duty, neglect, error, misstatement, misleading statements or omission, solely for acts or omissions committed by Contractor; all due to Contractor's negligence in providing professional services to Contractor customers. This includes coverage for loss of intangible property (such as customer data). The policy includes coverage for network security, unauthorized access, unauthorized use, receipt or transmission of a malicious code, denial of service attack, unauthorized disclosure or misappropriation of private information and privacy liability. It also includes notification costs, credit card monitoring, and fines & penalties incurred by the customer due to Contractor's mistake or error. Coverage includes network security and privacy liability.

e. Crime/Employee Fidelity Insurance

1) The Contractor shall maintain insurance, covering loss of money, securities and other tangible property belonging to State resulting directly from a fraudulent or dishonest act by a Contractor employee, by any means including a computer, while performing Contractor's professional services for the State. State shall be included as a loss payee under this policy. Contractor will continue its insurance coverages for the term of this contract and for a duration of two years after

expiration, as long as such coverage remains commercially available in the market place. This insurance shall have a minimum per claim of $5,000,000.

D.33. Major Procurement Contract Sales and Use Tax. Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.

D.34. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. The Contractor shall only use Confidential Information for activities pursuant to and related to the performance of the Contract. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

D.35. The obligations set forth in this Section shall survive the termination of this Contract. Equal Opportunity. The Contractor agrees as follows:

a. The Contractor will not discriminate against any employee or applicant for employment because of disability, race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their disability, race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

(1) Employment, upgrading, demotion, or transfer, recruitment or recruitment advertising;

(2) Layoff or termination;

(3) Rates of pay or other forms of compensation; and

(4) Selection for training, including apprenticeship.

The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

b. The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive considerations for employment without regard to disability, race, color, religion, sex, sexual orientation, gender identity, or national origin.

c. If the State approves any subcontract, the subcontract shall include paragraphs (a) and (b) above.

d. In addition, to the extent applicable the Contractor agrees to comply with 41 C.F. R. § 60-1.4, as that section is amended from time to time during the term.

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. State Ownership of Goods. The State shall have ownership, right, title, and interest in all goods provided by Contractor under this Contract including full rights to use the goods and transfer title in the goods to any third parties, as outlined in 42 CFR §433, inclusive of all subsections, and State Medicaid Director letter 18-005 or the most recent guidance.

E.3. Additional lines, items, or options. At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.

a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:

(1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;

(2) Any pricing related to the new lines, items, or options;

(3) The expected effective date for the availability of the new lines, items, or options; and

(4) Any additional information requested by the State.

b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.

c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.

d. Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

E.4. Intellectual Property Indemnity. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

In addition to the above indemnity, if the State's use of any deliverable, or any portion thereof, provided under this Contract, is or is likely to be enjoined by order of a court of competent jurisdiction as such an infringement or unauthorized use, the Contractor, at its expense, shall: (i) procure for the State the continued use of such deliverable; (ii) replace such deliverable with a non-infringing counterpart; or (iii) modify such deliverable so it becomes non-infringing; provided that, if (ii) or (iii) is the option chosen by the Contractor, the replacement or modified deliverable must be capable of performing substantially the same function. Notwithstanding the foregoing, the State retains the right to terminate the Contract in accordance with Section D.5 hereunder in the event of such infringement or unauthorized use, and any such exercise of these allowable options by Contractor shall not relieve Contractor of its indemnity obligations under this Section.

The forgoing indemnity does not apply to the extent that the infringement arises from: (i); items not provided by Contractor State's use of the deliverable not in accordance with instructions, documentations, or specifications ("Misuse"); (ii) State's alteration, modification or revision of the Deliverables not expressly authorized by the Contractor ("Alteration"); (iii) State's

failure to use or implement corrections or enhancements to the Deliverables made available by the Contractor to the State at no additional cost to the State, except where such failure to use or implement corrections or enhancements is a result of State's termination in accordance with the preceding paragraph; or (iv) State's combination of the Deliverables with materials not provided, specified, or approved by the Contractor.

E.5. Software License Warranty. Contractor grants a license to the State to use all software provided under this Contract in the course of the State's business and purposes. The Solution will contain Contractor COTS offerings, both SaaS and programs, as well as third-party COTS offerings. The list of such COTS offerings and their applicable terms and conditions can be found in Attachment H (the "EULA"). The State agrees to comply with such terms and conditions when using or accessing those COTS offerings PROVIDED THAT any provision in the EULA or any third party provider agreement containing the following shall be null, void, and unenforceable against the State: (i) any provision requiring the State to indemnify any entity; (ii) any provision regarding confidentiality obligations that are contrary to the Tennessee Public Records Act; (iii) any provision requiring the State to pay taxes or reimburse any entity for tax payments; (iv) any provision requiring the State to submit to any alternative dispute resolution; (v) any provision allowing collection of attorneys fees or late payments against the State other than as allowed under the Tennessee Prompt Pay Act; Tenn. Code Ann. § 12-4-701, et seq.; (vi) any provision allowing equitable or injunctive relief against the State; and (vii) any provision that is illegal to include in a contract with the State of Tennessee, to enforce against the State of Tennessee, or otherwise contravenes Tennessee or federal law. In no event shall any provision in the EULA or any third party provider agreements be considered a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, or any other immunity based on the Eleventh Amendment to the Constitution of the United States or State of Tennessee Constitution, or any remedies available to the State at law, from any claim or from the jurisdiction of any court, and any such terms and conditions are void, invalid, and unenforceable against the State. Moreover, in the event of any conflict between the terms and conditions of this Contract and the terms and conditions of any EULA or third party provider agreement, the terms and conditions of this Contract shall prevail.

E.6. Software Support and Maintenance Warranty. Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its customers.

E.7. Extraneous Terms and Conditions. Contractor shall fill all orders submitted by the State under this Contract. No purchase order, invoice, or other documents associated with any sales, orders, or supply of any good or service under this Contract shall contain any terms or conditions other than as set forth in the Contract. Any such extraneous terms and conditions shall be void, invalid and unenforceable against the State. Any refusal by Contractor to supply any goods or services under this Contract conditioned upon the State submitting to any extraneous terms and conditions shall be a material breach of the Contract and constitute an act of bad faith by Contractor.

E.8. Transfer of Ownership of Custom Software Developed for the State.

a) Definitions.

1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.

2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State under this Contract intended to function with the Contractor-Owned Software or any Work Product provided under this Contract.

3) "Rights Transfer Application Software," shall mean any pre-existing application software and documentation owned or supplied by Contractor or a third party necessary for the use, functioning, support, or maintenance of the Contractor-Owned

Software, the Custom-Developed Application Software, Third Party Software, and any Work Product provided to State.

4) "Third-Party Software," shall mean software supplied by Contractor under this Contract or necessary for the functioning of any Work Product not owned by the State or the Contractor.

5) "Work Product," shall mean all deliverables such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State under this Contract. Work Product shall include Rights Transfer Application Software.

b) Rights and Title to the Software

1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license or transfer of rights or ownership granted under this Contract. Contractor grants the State a perpetual non-exclusive license to the Contractor-Owned Software to be used solely with the Custom-Developed Application Software and the Work Product.

2) Contractor shall provide the source code in the Custom-Developed Application Software and, Work Product, with all subsequent modifications, enhancements, bug-fixes or any other changes in the source code of the Work Product and all other code and documentation necessary for the Custom-Developed Application Software to be installed and function as intended and as set forth in this Contract, to the State.

3) Contractor may lease or sell the Custom-Developed Application Software to third parties with the written permission of the State, which permission may be conditioned on the State receiving royalties from such sales or licenses.

4) All right, title and interest in and to the Custom-Developed Application Software, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other intellectual property and other proprietary rights embodied by and arising out of the Custom-Developed Application Software, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Custom-Developed Application Software, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Custom-Developed Application Software. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties. The State grants to the Contractor an irrevocable, nonexclusive, worldwide, fully paid up, perpetual license to make, have made, use, have used, lease, sell, offer to sell, license, import, or otherwise transfer, or practice any method covered by the Custom-Developed Application Software; provided that the Contractor shall not charge future government customers receiving CMS FFP for the use, development and design of such Custom-Developed Application Software and the Contractor complies with all requirements of this contract and applicable law, including CMS regulations, with respect to such future government customers receiving CMS FFP.

5) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted under this Contract.

c) The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others, materials which are similar to or competitive with those that are produced under this Contract.

d) To the extent that the Contractor uses any of its pre-existing, proprietary or independently developed tools, computer code, templates, materials or information, including Contractor-Owned Software, the Contractor shall retain all right, title and interest in and to such materials, and all modifications, derivatives and enhancements thereto (except to the

extent including the State's Confidential Information or Confidential State Data) and the State shall acquire no ownership right, title or interest in or to such materials EXCEPT the Contractor grants to the State a limited, non-transferable license to use, copy and distribute, solely for the State's internal purposes, any such materials necessary for the functioning or operation of any Work Product provided under the Contract.

e) Notwithstanding anything to the contrary in this Section, the State shall have all ownership rights in software or modifications thereof and associated documentation that is designed, developed, installed, or improved hereunder with Federal Financial Participation under 45 C.F.R. 95.617 and 45 C.F.R. 92.34, and the Federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal Government purposes, such software, modification, and documentation.

E.9. Contractor Hosted Services Confidential Data, Audit, and Other Requirements

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.

3) The Contractor shall maintain a Security Management Certification from the Federal Risk and Authorization Management Program ("FedRAMP"). A "Security Management Certification" shall mean written confirmation from FedRAMP that FedRAMP has assessed the Contractor's information technology Infrastructure, using a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, and has certified that the Contractor meets FedRAMP standards. Information technology "Infrastructure" shall mean the Contractor's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services. The Contractor shall provide proof of current certification annually and upon State request. No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

Contractor shall meet all applicable requirements of the most current version of Internal Revenue Service Publication 1075.

Contractor shall meet requirements of current version of Minimum Acceptable Risk Standards for Exchanges ("MARS-E") controls.

4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.

6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies. The State's Enterprise Information Security Policies document is attached to this Contract at Attachment C, Procurement Library.

2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

   i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: 24 hours for the EDW, DSS, and DQ/ETL Pipeline Component; 10 minutes for the MDM Component

   ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: 24 hours for the EDW, DSS, and DQ/ETL Pipeline Component; 4 hours for the MDM Component

2) The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

e. The Contractor and any Subcontractor used by the Contractor to host State data, including data center vendors, shall be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide the State with the Contractor's and Subcontractor's annual audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor and Subcontractor.

   If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

   No additional funding shall be allocated for these audits as they are included in the Maximum Liability of this Contract.

E.10. State Furnished Property. The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less reasonable wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.

E.11. Work Papers Subject to Review**.** The Contractor shall make all audit, accounting, or financial analysis work papers, notes, and other documentation available for review by the Comptroller of the Treasury or his representatives, upon request, during normal working hours either while the analysis is in progress or subsequent to the completion of this Contract.

E.12. Prohibited Advertising or Marketing**.** The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.13. Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:

a) No federally appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

b) If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying,'' in accordance with its instructions.

c) The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by 31 USC § 1352.

E.14. Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to Solicitation Number **31865-00619** (Attachment 6.2 Section B, Section B.17) and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a monthly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, service-disabled veterans, and persons with disabilities. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the TN Diversity Software available online at: https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9810.

E.15. Liquidated Damages. In the event of a Contract performance or compliance failure by the Contractor, the State may, but is not obligated to address such Contract performance failure and/or assess damages ("Liquidated Damages") in accordance with Attachment B, Service Level Agreement and Liquidated Damages for DQ/ETL of the Contract. The State shall notify the Contractor of any amounts to be assessed as Liquidated Damages via the Control Memorandum process specified in Contract Section A.12.8. The Parties agree that due to the complicated nature of the Contractor's obligations under this Contract it would be difficult to specifically designate a monetary amount for a Contract performance or compliance failure, as these amounts are likely to be uncertain and not easily proven. Contractor has carefully reviewed the Liquidated Damages contained in Contract Attachment B, Service Level Agreements and Liquidated Damages for DQ/ETL and agrees that these amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of a Contract performance or compliance failure, are reasonable estimates of the damages that would occur from a Contract performance or compliance failure, and are not punitive. The Parties agree that although the Liquidated Damages represent the reasonable estimate of the damages and injuries sustained by the State due to the Contract performance or compliance failure, they do not include any injury or damage sustained by a third party. The Contractor agrees that the Liquidated Damages are in addition to any amounts Contractor may owe the State pursuant to the indemnity provision or any other sections of this Contract.

The State is not obligated to assess Liquidated Damages as a result of a Contract performance or compliance failure before availing itself of any other remedy. In the event of multiple Contract performance or compliance failures, the Parties recognize that the cumulative effect of these Contract performance failures may exceed the compensation provided by Liquidated Damages. The State may choose to avail itself of any other remedy available under this Contract or at law or equity. The Parties further recognize that the State may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

Without regard to whether the State has imposed Liquidated Damages or pursued any other remedy due to any action or inaction by the Contractor, the State may impose a corrective action plan or similar measure through a Control Memorandum. Such measure is neither punitive nor related to any damages the State might suffer.

E.16. Partial Takeover of Contract**.** The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a "Partial Takeover"). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State's exercise of a Partial Takeover shall not alter the Contractor's other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State's exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State's exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.

E.17. End of Contract Turnover Plan. As part of the transition of this Contract to a new vendor when this Contract ends, if applicable, the Contractor shall develop and provide to the State a Turnover Plan no later than one hundred and eighty (180) days prior to the Contract end date. The Turnover Plan shall contain the information requested by TennCare in a Control Memorandum as described in Section A.12.8.

E.18. Turnover Requirements. Prior to the end of the Contract term or extension of the Contract term, or in the event of a Contract Termination or Partial Takeover pursuant to Contract Sections pertaining to "Termination for Cause", "Termination for Convenience", and "Partial Takeover of Contract", the State may contract with a successor contractor (Successor Contractor) to assume the Contactor's duties and requirements upon termination of this Contract. This may result in a period of transition during which the Contractor continues to provide services while the Successor Contractor prepares to assume those services, with a switch over from the Contractor to the Successor Contractor occurring on an implementation date specified by the State. The Contractor shall be required to participate as directed by the State, at no additional cost, in assisting with the transition by providing information relating to the Contractor's duties and attending meetings with the State and/or Successor Contractor. The Contractor shall help the State and/or the Successor Contractor develop a comprehensive Turnover Plan covering both the Contractor's and the Successor Contractor's duties and responsibilities to ensure a smooth transition of responsibilities. The Contractor shall, at all times, act in good faith toward the State and/or Successor Contractor to facilitate as smooth a transition as possible. The State will use the Control Memorandum process (as described in Section A.12.8) to specify deliverables required of the Contractor in aid of the transition process. Failure to fully and timely cooperate with the State's request or provide the requested deliverables may result in liquidated damages as specified in this Contract or in the applicable Control Memorandum. . The State shall not be liable to the Contractor for any costs and expenses relating to these deliverables or to the services provided by the Contractor during the transition period, other than as set forth in Contract Section C.

E.19. Unencumbered Personnel**.** The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Contract from performing the same or similar services for the State after the termination of this Contract,

either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

E.20. Personally Identifiable Information**.** While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within forty-eight (48) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure, and shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, and any mitigation, including individual letters and public notice, where the Unauthorized Disclosure was caused by acts or omissions of Contractor, Contractor personnel or Contractor subcontractors or by Contractor's failure to perform Contractor's obligations under this Contract, including Contractor's data security obligations ("Contractor Fault"). If an Unauthorized Disclosure occurs that was not due to Contractor Fault, Contractor shall bear the cost of credit monitoring services and any mitigation, including notification to individuals affected by the Unauthorized Disclosure, up to $10,000,000, except to the extent that the Unauthorized Disclosure was caused by a State employee or a State contractor. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.

E.21. Federal Funding Accountability and Transparency Act (FFATA). This Contract requires the Contractor to provide supplies or services that are funded in whole or in part by federal funds that are subject to FFATA. The Contractor is responsible for ensuring that all applicable requirements, including but not limited to those set forth herein, of FFATA are met and that the Contractor provides information to the State as required.

The Contractor shall comply with the following:

a) Reporting of Total Compensation of the Contractor's Executives.

1) The Contractor shall report the names and total compensation of each of its five most highly compensated executives for the Contractor's preceding completed fiscal year, if in the Contractor's preceding fiscal year it received:

    i) 80 percent or more of the Contractor's annual gross revenues from federal procurement contracts and federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

    ii) $25,000,000 or more in annual gross revenues from federal procurement contracts (and subcontracts), and federal financial assistance subject to the Transparency Act (and subawards); and

    iii) The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 USC 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986. (To determine if the public has access to the compensation information, see the U.S. Security and Exchange Commission total compensation filings at http://www.sec.gov/answers/execomp.htm).

    As defined in 2 C.F.R. § 170.315, "Executive" means officers, managing partners, or any other employees in management positions.

b) Total compensation means the cash and noncash dollar value earned by the executive during the Contractor's preceding fiscal year and includes the following (for more information see 17 C.F.R. § 229.402l(2)):

    i) Salary and bonus.

    ii) Awards of stock, stock options, and stock appreciation rights. Use the dollar amount recognized for financial statement reporting purposes with respect to the fiscal year in accordance with the Statement of Financial Accounting Standards No. 123 (Revised 2004) (FAS 123R), Shared Based Payments.

    iii) Earnings for services under non-equity incentive plans. This does not include group life, health, hospitalization or medical reimbursement plans that do not discriminate in favor of executives, and are available generally to all salaried employees.

    iv) Change in pension value. This is the change in present value of defined benefit and actuarial pension plans.

    v) Above-market earnings on deferred compensation which is not tax qualified.

    vi) Other compensation, if the aggregate value of all such other compensation (e.g. severance, termination payments, value of life insurance paid on behalf of the employee, perquisites or property) for the executive exceeds $10,000.

c) The Contractor must report executive total compensation described above to the State by the end of the month during which this Contract is awarded.

d) If this Contract is amended to extend the Term, the Contractor must submit an executive total compensation report to the State by the end of the month in which the term extension becomes effective.

e) The Contractor will obtain a Data Universal Numbering System (DUNS) number and maintain its DUNS number for the term of this Contract. More information about obtaining a DUNS Number can be found at: http://fedgov.dnb.com/webform/

The Contractor's failure to comply with the above requirements is a material breach of this Contract for which the State may terminate this Contract for cause. The State will not be obligated to pay any outstanding invoice received from the Contractor unless and until the Contractor is in full compliance with the above requirements.

E.22. Drug-Free Workplace. The Contractor shall provide a drug-free workplace pursuant to the Drug-Free Workplace Act of 1988, Title 41 U.S.C. §§ 701, *et seq.*, and the regulations in Title 41 U.S.C.A. §§ 8101 through 8106.

E.23. Survival. The terms, provisions, representations, and warranties contained in this Contract which by their sense and context are intended to survive the performance and termination of this Contract, shall so survive the completion of performance and termination of this Contract.

E.24. Applicable Laws, Rules, Policies and Court Orders. The Contractor agrees to comply with all applicable federal and State laws rules, regulations, sub-regulatory guidance including but not limited to the State Medicaid Manual, executive orders, TennCare waivers, and all current, modified or future Court decrees, orders or judgments applicable to the State's TennCare and CHIP programs. Such compliance shall be performed at no additional cost to the State.

E.25. Business Associate. As the Contractor will provide services to TennCare pursuant to which the Contractor will have access to, receive from, create, or receive on behalf of TennCare Protected Health Information, or Contractor will have access to, create, receive, maintain or transmit on behalf of TennCare Electronic Protected Health Information (as those terms are defined under HIPAA and HITECH), Contractor hereby acknowledges its designation as a business associate under HIPAA and agrees to comply with all applicable HIPAA regulations and any further responsibilities set forth in the Business Associate Agreement (See Attachment F) between the Parties.

E.26. Notification of Breach and Notification of Suspected Breach. The Contractor shall notify TennCare's Privacy Office immediately upon becoming aware of and in no case later than forty-eight (48) hours after discovery of any incident, either confirmed or suspected, that represents or may represent unauthorized access, use or disclosure of encrypted or unencrypted computerized data that materially compromises the security, confidentiality, or integrity of enrollee PHI maintained or held by the Contractor, including any unauthorized acquisition of enrollee PHI by an employee or otherwise authorized user of the Contractor 's system. This includes, but is not limited to, loss or suspected loss of remote computing or telework devices such as laptops, PDAs, Blackberrys or other Smartphones, USB drives, thumb drives, flash drives, CD-Rs, and/or disks.

E.27. Transmission of Contract Deliverables. All information or data that is necessary for one or more deliverable set forth in this Contract shall be transmitted between TennCare and Contractor via the data transfer method specified in advance by TennCare. This may include, but shall not be limited to, transfer through TennCare's SFTP system. Failure by the Contractor to transmit information or data that is necessary for a deliverable in the manner specified by TennCare, may, at the option of TennCare, result in liquidated damages as set forth in Contract Attachment B – Service Level Agreements and Liquidated Damages for DQ/ETL.

E.28. Social Security Administration (SSA) Required Provisions for Data Security. The Contractor shall comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 USC 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 USC §3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the Contractor shall have in place administrative, physical, and technical safeguards for data.

a) The Contractor shall specify in its agreements with any agent or subcontractor that will have access to data that such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to the Contractor pursuant to this Section.

b) The Contractor shall not duplicate in a separate file or disseminate, without prior written permission from TennCare, the data governed by the Contract for any purpose other than that set forth in this Contract for the administration of the TennCare program. Should the Contractor propose a redisclosure of said data, the Contractor must specify in writing to TennCare the data the Contractor proposes to redisclose, to whom, and the reasons that justify the redisclosure. TennCare will not give permission for such redisclosure unless the redisclosure is required by law or essential to the administration of the TennCare program.

c) The Contractor agrees to abide by all relevant federal laws, restrictions on access, use, and disclosure, and security requirements in this Contract.

d) The Contractor shall provide a current list of the employees of such contractor with access to SSA data and provide such lists to TennCare upon request and at any time there are changes.

e) The Contractor shall restrict access to the data obtained from TennCare to only those authorized employees who need such data to perform their official duties in connection with purposes identified in this Contract. The Contractor shall not further duplicate, disseminate, or disclose such data without obtaining TennCare's prior written approval.

f) The Contractor shall ensure that its employees:

1) Properly safeguard SSA-supplied data furnished by TennCare under this Contract from loss, theft or inadvertent disclosure;

2) Receive regular, relevant and sufficient SSA data related training, including use, access and disclosure safeguards and information regarding penalties for misuse of information;

3) Understand and acknowledge that they are responsible for safeguarding this information at all times, regardless of whether or not the Contractor employee is at his or her regular duty station;

4) Ensure that laptops and other electronic devices/media containing SSA-supplied data are encrypted and/or password protected;

5) Send emails containing SSA-supplied data only if encrypted or if to and from addresses that are secure; and,

6) Limit disclosure of the information and details relating to a SSA-supplied data loss only to those with a need to know.

Contractor employees who access, use, or disclose TennCare or TennCare SSA-supplied data in a manner or purpose not authorized by this Contract may be subject to civil and criminal sanctions pursuant to applicable federal statutes.

g) Loss or Suspected Loss of Data–If an employee of the Contractor becomes aware of suspected or actual loss of SSA-supplied data, the Contractor must immediately contact TennCare immediately upon becoming aware to report the actual or suspected loss. The Contractor must provide TennCare with timely updates as any additional information about the loss of SSA-supplied data becomes available.

If the Contractor experiences a loss or breach of said data, TennCare will determine whether or not notice to individuals whose data has been lost or breached shall be provided and the Contractor shall bear any costs associated with the notice or any mitigation where the loss or breach of said data was caused by acts or omissions of Contractor, Contractor personnel or Contractor subcontractors or by Contractor's failure to perform Contractor's obligations under this Contract, including Contractor's data security obligations ("Contractor Fault"). If a loss or breach of data occurs that was not due to Contractor Fault, Contractor shall bear the cost of notice or any mitigation, including notification to individuals affected by the loss or breach of said data, up to $10,000,000, except to the extent that the loss or breach of said data was caused by a State employee or a State contractor .

h) TennCare may immediately and unilaterally suspend the data flow under this Contract, or terminate this Contract, if TennCare, in its sole discretion, determines that the Contractor has: (1) made an unauthorized use or disclosure of TennCare SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this Contract.

i) This Section further carries out Section 1106(a) of the Act (42 USC 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy of 1974 (5 USC 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budge" ("MB") guidelines, the Federal Information Security Management Act of 2002 (44 USC 3541 et seq.), and related National Institute of

Standards and Technology ("NIST") guidelines, which provide the requirements that the SSA stipulates that the Contractor must follow with regard to use, treatment, and safeguarding data in the event data is exchanged with a federal information system.

j) Definitions

1) "SSA-supplied data" or "data" as used in this section means an individual's personally identifiable information (e.g. name, social security number, income), supplied by the Social Security Administration to TennCare to determine entitlement or eligibility for federally-funded programs pursuant to a Computer Matching and Privacy Protection Act Agreement and Information Exchange Agreement between SSA and the State of Tennessee.

E.29. Medicaid and CHIP. The Contractor must provide safeguards that restrict the use or disclosure of information concerning applicants and beneficiaries to purposes directly connected with the administration of the plan:

a) Purposes directly related to the administration of Medicaid and CHIP include:

1) establishing eligibility;

2) determining the amount of medical assistance;

3) providing services for beneficiaries; and,

4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to Medicaid or CHIP administration.

b) The Contractor must have adequate safeguards to assure that:

1) Information is made available only to the extent necessary to assist in the valid administrative purposes of those receiving the information, and information; and

2) received under 26 USC is exchanged only with parties authorized to receive that information under that section of the Code; and, the information is adequately stored and processed so that it is protected against unauthorized disclosure for other purposes.

c) The Contractor must have criteria that govern the types of information about applicants and beneficiaries that are safeguarded. This information must include at least:

1) Names and addresses;

2) Medical services provided;

3) Social and economic conditions or circumstances;

4) Contractor evaluation of personal information;

5) Medical data, including diagnosis and past history of disease or disability

6) Any information received for verifying income eligibility and amount of medical assistance payments, including income information received from SSA or the Internal Revenue Service;

7) Income information received from SSA or the Internal Revenue Service must be safeguarded according to Medicaid and CHIP requirements;

8) Any information received in connection with the identification of legally liable third party resources; and.

9) Social Security Numbers.

d) The Contractor must have criteria approved by TennCare specifying:

1) The conditions for release and use of information about applicants and beneficiaries;

2) Access to information concerning applicants or beneficiaries must be restricted to persons or Contractor representatives who are subject to standards of confidentiality that are comparable to those of TennCare;

3) The Contractor shall not publish names of applicants or beneficiaries;

4) The Contractor shall obtain permission from a family or individual, whenever possible, before responding to a request for information from an outside source, unless the information is to be used to verify income, eligibility and the amount of medical assistance payment to an authorized individual or entity;

5) If, because of an emergency situation, time does not permit obtaining consent before release, the Contractor shall notify TennCare, the family or individual immediately after supplying the information.

6) The Contractor's policies must apply to all requests for information from outside sources, including governmental bodies, the courts, or law enforcement officials.

   i. The Contractor shall notify TennCare of any requests for information on applicants or beneficiaries by other governmental bodies, the courts or law enforcement officials ten (10) days prior to releasing the requested information.

7) If a court issues a subpoena for a case record or for any Contractor representative to testify concerning an applicant or beneficiary, the Contractor must notify TennCare at least ten (10) days prior to the required production date so TennCare may inform the court of the applicable statutory provisions, policies, and regulations restricting disclosure of information.

8) The Contractor shall not request or release information to other parties to verify income, eligibility and the amount of assistance under Medicaid or CHIP, prior to express approval from TennCare.

E.30. Employees Excluded from Medicare, Medicaid or CHIP. The Contractor does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly employ, in the performance of this Contract, employees who have been excluded from participation in the Medicare, Medicaid, and/or CHIP programs pursuant to Sections 1128 of the Social Security Act. All employees shall be screened against the HHS-OIG LEIE and GSA SAM databases prior to beginning to work on the project covered by this Contract.

E.31. Offer of Gratuities. By signing this Contract, the Contractor signifies that no member of or a delegate of Congress, nor any elected or appointed official or employee of the State of Tennessee, the federal General Accounting Office, federal Department of Health and Human Services, the CMS, or any other state or federal agency has or will benefit financially or materially from this Contract. This Contract may be terminated by TennCare as provided in Section D.6, if it is determined that gratuities of any kind were offered to or received by any of the aforementioned officials or employees from the Contractor, its agent, or employees.

E.32. Internal Revenue Service (IRS) Safeguarding Of Return Information:

a) Performance – In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1) This provision shall not apply if information received or delivered by the Parties under this Contract is NOT "federal tax returns or return information" as defined by IRS Publication 1075 and IRC 6103.

2) All work will be done under the supervision of the Contractor or the Contractor's employees. The Contractor and the Contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.

4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

5) The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to TennCare or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide TennCare or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

7) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

8) No work involving Federal tax information furnished under this Contract will be subcontracted without prior written approval of the IRS.

9) The Contractor will maintain a list of employees authorized access. Such list will be provided to TennCare and, upon request, to the IRS reviewing office.

10) TennCare will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

b) Criminal/Civil Sanctions

1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found

liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 USC 552a. Specifically, 5 USC 552a(i)(1), which is made applicable to contractors by 5 USC 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

4) Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Publication 1075 Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Publication 1075 Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Publication 1075 Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

   Inspection – The IRS and TennCare, with twenty-four (24) hours' notice, shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work with FTI under this Contract. The IRS and TennCare's right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safe.

E.33. Discovery and Litigation Hold Requirements. TennCare is frequently involved in litigation as either a party or a non-party with relevant information. Contractor shall cooperate with all TennCare requests to aid in data and document retention, and collection, as required for litigation. Contractor will also provide subject matter experts as needed for depositions or as witnesses at trial. These services will be provided at no cost to the state. TennCare and its attorneys will exert all reasonable efforts to limit the scope and cost of discovery and litigation requests.

E.34. Litigation Support. If any litigation should arise that requires the defense of a TennCare claim before any court or tribunal, the Contractor shall cooperate fully and timely with any TennCare Office of General Counsel (OGC) attorneys or paralegals in defense of the claim at no additional cost to the State. The Contractor shall make its personnel available to testify in Tennessee, whether in person before a tribunal or by deposition. The Contractor agrees to waive any objections to any subpoena issued by a Tennessee tribunal, in a case related to this Contract. The Contractor shall promptly provide OGC with all information within the Contractor's control if required to do so by a discovery demand or court order.

E.35. Nondiscrimination Compliance Requirements.

a) The Contractor shall comply with all applicable federal and state civil rights laws, regulations, rules, and policies, which may include, but are not limited to, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990,

the Age Discrimination Act of 1975, and 42 U.S.C. § 18116 (codified at 45 C.F.R. pt. 92) and Contract Section D.9.

b) Records. The Contractor shall keep such records as may be necessary in order to submit timely, complete, and accurate compliance reports that may be requested by the U.S. Department of Health and Human Services (HHS), the U.S. Department of Justice (DOJ), TennCare, and the Tennessee Human Rights Commission (THRC) or their designees. If requested, the information shall be provided in a format and timeframe specified by HHS, DOJ, TennCare, or THRC. The requested information may be necessary to enable HHS, DOJ, TennCare, or THRC to ascertain whether the Contractor is complying with the applicable civil rights laws. For example, the Contractor should have available data showing the manner in which services are or will be provided by the program in question, and related data necessary for determining whether any persons are or will be denied such services on the basis of prohibited discrimination. Further examples of data that could be requested can be found at 45 C.F.R. § 80.6 and 28 C.F.R. § 42.406.

c) Access. The Contractor shall permit access as set forth in the applicable civil rights laws, such as, 45 C.F.R. § 80.6 to HHS, DOJ, TennCare, and THRC or their designees during normal business hours to such of its books, records, accounts, and other sources of information, and its facilities as may be pertinent to ascertain whether the Contractor is complying with the applicable civil rights laws.

d) Discrimination Complaint Investigations. In the event, a discrimination complaint is filed by either a TennCare employee or a Contractor staff member alleging an incident claimed to be caused by either the Contractor's staff or one of its subcontractors who are considered to be performing duties under this contact, the Contractor shall cooperate with TennCare's Office of Civil Rights Compliance (OCRC) during the investigation and resolution of the complaint allegation. Should the Contractor receive a report of a discrimination complaint allegation related to the activities being performed under this contract, the Contractor shall inform OCRC of the complaint within two (2) Business Days from the date Contractor learns of the complaint, OCRC shall determine the complaint investigation outcome, resolution, and/or corrective action.

e) Electronic and Information Technology Accessibility Requirements. In fulfilling its responsibility under this Contract, the Contractor shall comply with the civil rights requirements set forth in A.9.2 regarding incorporating the accessibility requirements into the design, development, installation, and enhancement of Electronic and Information Technology. For any user interfaces, the Contractor shall include a link to TennCare's Notice of Nondiscrimination and Language Help Notice.

f) Training. On an annual basis, the Contractor shall be responsible for making nondiscrimination training available to all Contractor staff and to its subcontractors that are considered to be recipients of federal financial assistance under this contract. The Contractor shall be able to show documented proof to OCRC that the training was made available to the Contractor's staff and to its subcontractors that are considered to be recipients of federal financial assistance under this contract.

IN WITNESS WHEREOF,

INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM):

Craig E Haseltine — 6/3/2022

CONTRACTOR SIGNATURE **DATE**

Craig E. Haseltine, VP

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF FINANCE AND ADMINISTRATION
DIVISION OF TENNCARE:

Jim Bryson

Digitally signed by Jim Bryson
Date: 2022.07.28 09:49:06 -05'00'

JIM BRYSON, COMMISSIONER **DATE**

CONTRACT ATTACHMENT A

DEFINITIONS AND ABBREVIATIONS

Located in the Procurement Library

CONTRACT ATTACHMENT B

SERVICE LEVEL AGREEMENTS AND LIQUIDATED DAMAGES for DQ/ETL

Located in the Procurement Library

CONTRACT ATTACHMENT C

PROCUREMENT LIBRARY

CONTRACT ATTACHMENT D

REQUIREMENTS TRACEABILITY OVERVIEW AND MATRIX

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	
EDISON VENDOR IDENTIFICATION NUMBER:	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

Craig E Haseltine

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Craig E. Haseltine, VP

PRINTED NAME AND TITLE OF SIGNATORY

6/3/2022

DATE OF ATTESTATION

Division of TennCare

HIPAA Business Associate Agreement

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT ("Agreement") is between The State of Tennessee, Division of TennCare ("TennCare" or "Covered Entity"), located at 310 Great Circle Road, Nashville, TN 37243 and IBM Corporation ("Business Associate"), located at 1 New Orchard Road, Armonk, NY 10504, including all office locations and other business locations at which Business Associate data may be used or maintained. Covered Entity and Business Associate may be referred to herein individually as "Party" or collectively as "Parties."

BACKGROUND

The Parties acknowledge that they are subject to the Privacy and Security Rules (45 C.F.R. Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and as amended by the final rule modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (HITECH). If Business Associate provides services to Covered Entity pursuant to one or more contractual relationships, said Agreements are detailed below and hereinafter referred to as "Service Agreements."

LIST OF AGREEMENTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT:

In the course of performing services under a Service Agreement, Business Associate may come into contact with, use, or disclose Protected Health Information ("PHI"). Said Service Agreements are hereby incorporated by reference and shall be taken and considered as a part of this document the same as if fully set out herein.

In accordance with the federal privacy and security rules and regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A, C, D and E, which require Covered Entity to have a written memorandum with each of its Business Associates, the Parties wish to establish satisfactory assurances that Business Associate will appropriately safeguard PHI that Business Associate may receive (if any) from or on behalf of Covered Entity, and, therefore, execute this Agreement.

1. DEFINITIONS

All capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms defined in 45 C.F.R. Parts 160 through 164 or other applicable law or regulation. A reference

in this Agreement to a section in the Privacy or Security Rule means the section as in effect or as amended.

1.1 "Commercial Use" means obtaining PHI with the intent to sell, transfer or use it for commercial, or personal gain, or malicious harm; sale to third party for consumption, resale, or processing for resale; application or conversion of data to make a profit or obtain a benefit contrary to the spirit of this Agreement, including but not limited to presentation of data or examples of data in a conference or meeting setting where the ultimate goal is to obtain or gain new business.
1.2 "Confidential Information" shall mean any non-public, confidential or proprietary information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, which is supplied by TennCare to the Business Associate under this Agreement. Any information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, relating to individuals enrolled in the TennCare program ("TennCare enrollees"), or relating to individuals who may be potentially enrolled in the TennCare program, which is provided to or obtained through the Business Associate's performance under this Agreement, shall also be treated as "Confidential Information" to the extent that confidential status is afforded such information under state and federal laws or regulations. All confidential information shall not be subject to disclosure under the Tennessee Public Records Act.

1.3 "Electronic Signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

1.4 "Marketing" shall have the meaning under 45 C.F.R. § 164.501 and the act or process of promoting, selling, leasing or licensing any TennCare information or data for profit without the express written permission of TennCare.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Privacy Rule)

2.1 Compliance with the Privacy Rule. Business Associate shall fully comply with the requirements under the Privacy Rule applicable to "business associates," as that term is defined in the Privacy Rule and not use or further disclose PHI other than as permitted or required by this Agreement, the Service Agreements, or as required by law. In case of any conflict between this Agreement and the Service Agreements, this Agreement shall govern.

2.2 HITECH Act Compliance. The Health Information Technology for Economic and Clinical Health Act (HITECH) was adopted as part of the American Recovery and Reinvestment Act of 2009. HITECH and its implementing regulations impose new requirements on Business Associates with respect to privacy, security, and Breach notification. Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate shall comply with any applicable provisions of HITECH. Business Associate and the Covered Entity further agree that the provisions of HIPAA and HITECH that apply to business associates and that are required to be incorporated by reference in a business associate agreement have been incorporated into this Agreement between Business Associate and Covered Entity. Should any provision not be set forth specifically, it is as if set forth in this Agreement in its entirety and is effective as of the Applicable Effective Date, and as amended.

2.3 Business Management. Business Associate may use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate. Business Associate may provide data aggregation services relating to the Health Care Operations of TennCare, or as required by law. Business Associate is expressly prohibited from using or disclosing PHI other than as permitted by this Agreement, any associated Service Agreements, or as otherwise permitted or required by law, and is prohibited from uses or disclosures of PHI that would not be permitted if done by the Covered Entity.

2.4 Privacy Safeguards and Policies. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the Service Agreement(s), this Agreement or as required by law. This includes the implementation of Administrative, Physical, and Technical Safeguards to

reasonably and appropriately protect the Covered Entity's PHI against any reasonably anticipated threats or hazards, utilizing the technology commercially available to the Business Associate (See also Section 3.2). The Business Associate shall maintain appropriate documentation of its compliance with the Privacy Rule, including, but not limited to, its policies, and procedures, records of training and sanctions of members of its Workforce.

2.5 Business Associate Contracts. Business Associate shall require any agent, including a Subcontractor, to whom it provides PHI received from, maintained, created or received by Business Associate on behalf of Covered Entity, or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI or other confidential TennCare information, to agree, by written agreement with Business Associate, to substantially similar, but not less stringent restrictions and conditions that apply through this Agreement to Business Associate with respect to such information except for the provision at section 4.6, which shall only apply to the Business Associate notwithstanding the requirements in this section 2.5.

2.6 Mitigation of Harmful Effect of Violations. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

2.7 Reporting of Violations in Use and Disclosure of PHI. Business Associate shall require its employees, agents, and Subcontractors to promptly report to Business Associate immediately upon becoming aware of any use or disclosure of PHI in violation of this Agreement and to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement. The Business Associate shall report such violation to Covered Entity immediately upon becoming aware of, and in no case later than 48 hours after discovery.

2.8 Breach of Unsecured Protected Health Information. As required by the Breach Notification Rule, Business Associate shall, and shall require its Subcontractor(s) to, maintain systems to monitor and detect a Breach of Unsecured PHI, whether in paper or electronic form.

2.8.1 Business Associate shall provide to Covered Entity notice of a Breach of Unsecured PHI immediately upon becoming aware of the Breach, and in no case later than 48 hours after discovery.

2.8.2 Business Associate shall cooperate with Covered Entity in timely providing the appropriate and necessary information to Covered Entity.

2.8.3 Covered Entity shall make the final determination whether the Breach requires notification to affected individuals and whether the notification shall be made by Covered Entity or Business Associate.

2.9 Access of Individual to PHI and other Requests to Business Associate. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to provide access to PHI in a Designated Record Set to Covered Entity in order to meet its requirements under 45 C.F.R. § 164.524. If Business Associate receives a request from an Individual for a copy of the Individual's PHI, and the PHI is in the sole possession of the Business Associate, Business Associate will provide the requested copies to the Individual in a timely manner. If Business Associate receives a request for PHI not in its possession and in the possession of the Covered Entity, or receives a request to exercise other Individual rights as set forth in the Privacy Rule, Business Associate shall promptly forward the request to Covered Entity. Business Associate shall then assist Covered Entity as necessary in responding to the request in a timely manner. If a Business Associate provides copies of PHI to the Individual, it may charge a reasonable fee for the copies as the regulations shall permit.

2.10 Requests to Covered Entity for Access to PHI. The Covered Entity shall forward to the Business Associate in a timely manner any Individual's request for access to or a copy (in any form they choose,

provided the PHI is readily producible in that format) of their PHI that shall require Business Associate's participation, after which the Business Associate shall provide access to or deliver such information as follows:

(a) The Parties understand that if either Party receives a request for access to or copies of PHI from an Individual which the Party may complete with only its own onsite information, the time for such response shall be thirty (30) days, with notification to the Covered Entity upon completion.
(b) If the Covered Entity receives a request and requires information from the Business Associate in addition to the Covered Entity's onsite information to fulfill the request, the Business Associate shall have fifteen (15) days from date of Covered Entity's notice to provide access or deliver such information to the Covered Entity so that the Covered Entity may timely respond to the Individual within the thirty (30) day requirement of 45 C.F.R. § 164.524.
(c) If the Party designated above as responding to the Individual's request is unable to complete the response to the request in the time provided, that Party shall provide the Individual, or Individual's designee, with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Party may extend the response time once for no more than thirty (30) additional days.
(d) Business Associate is permitted to send an Individual or Individual's designee unencrypted emails including Electronic PHI if the Individual requests it, provided the Business Associate has advised the Individual of the risk and the Individual still prefers to receive the message by unencrypted email.

2.11 Individuals' Request to Amend PHI. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526, regarding an Individual's request to amend PHI. The Business Associate shall make the amendment promptly in the time and manner designated by Covered Entity, but shall have thirty (30) days' notice from Covered Entity to complete the amendment to the Individual's PHI and to notify the Covered Entity upon completion.

2.12 Recording of Designated Disclosures of PHI. Business Associate shall document any and all disclosures of PHI by Business Associate or its agents, including information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

2.13 Accounting for Disclosures of PHI. The Business Associate agrees to provide to Covered Entity or to an Individual, or Individual's designee, in time and manner designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. The Covered Entity shall forward the Individual's request requiring the participation of the Business Associate to the Business Associate in a timely manner, after which the Business Associate shall provide such information as follows:

(a) If Covered Entity directs Business Associate to provide an accounting of disclosures of the Individual's PHI directly to the Individual, the Business Associate shall have sixty (60) days from the date of the Individual's request to provide access to or deliver such information to the Individual or Individual's designee. The Covered Entity shall provide notice to the Business Associate in time to allow the Business Associate a minimum of thirty (30) days to timely complete the Individual's request.
(b) If the Covered Entity elects to provide the accounting to the Individual, the Business Associate shall have thirty (30) days from date of Covered Entity's notice of request to provide information for the Accounting to the Covered Entity so that the Covered Entity may timely respond to the Individual within the sixty (60) day period.
(c) If either of the Parties is unable to complete the response to the request in the times provided

above, that Party shall notify the Individual with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Parties may extend the response time once for no more than thirty (30) additional days.

(d) The accounting of disclosures shall include at least the following information:
(1) date of the disclosure;
(2) name of the third party to whom the PHI was disclosed,
(3) if known, the address of the third party;
(4) brief description of the disclosed information; and
(5) brief explanation of the purpose and basis for such disclosure.

(e) The Parties shall provide one (1) accounting in any twelve (12) months to the Individual without charge. The Parties may charge a reasonable, cost-based fee, for each subsequent request for an accounting by the same Individual if he/she is provided notice and the opportunity to modify his/her request. Such charges shall not exceed any applicable State statutes or rules.

2.14 Minimum Necessary. Business Associate shall use reasonable efforts to limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.

2.14.1 Business Associate represents to Covered Entity that all its uses and disclosures of, or requests for, PHI shall be the minimum necessary in accordance with the Privacy Rule requirements.

2.14.2 Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Business Associate.

2.14.3 Business Associate shall adequately and properly maintain all PHI received from, or created or received on behalf of, Covered Entity.

2.15 Privacy Compliance Review upon Request. Business Associate agrees to make its internal practices, books and records, including policies, procedures, and PHI, relating to the use and disclosure of PHI received from, created by or received by Business Associate on behalf of Covered Entity available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

2.16 Cooperation in Privacy Compliance. Business Associate agrees to fully cooperate in good faith and to assist Covered Entity in complying with the requirements of the Privacy Rule.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (Security Rule)

3.1 Compliance with Security Rule. Business Associate shall fully comply with the requirements under the Security Rule applicable to "Business Associates," as that term is defined in the Security Rule. In case of any conflict between this Agreement and Service Agreements, this Agreement shall govern.

3.2 Security Safeguards and Policies. Business Associate shall implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule. This includes specifically, but is not limited to, the utilization of technology commercially available at the time to the Business Associate to protect the Covered Entity's PHI against any reasonably anticipated threats or hazards. The Business Associate understands that it has an affirmative duty to perform a regular review or assessment of security risks, conduct active risk management and supply best efforts to assure that only authorized persons and devices access its computing systems and information storage, and that only authorized transactions are allowed. The Business Associate

will maintain appropriate documentation of its compliance with the Security Rule.

3.3 Security Provisions in Business Associate Contracts. Business Associate shall ensure that any agent to whom it provides Electronic PHI received from, maintained, or created for Covered Entity or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, shall execute a bilateral contract (or the appropriate equivalent if the agent is a government entity) with Business Associate, incorporating substantially similar, but not less stringent restrictions and conditions in this Agreement with Business Associate regarding PHI except for the provision in Section 4.6.

3.4 Reporting of Security Incidents. The Business Associate shall track all Security Incidents as defined and as required by HIPAA and shall periodically report such Security Incidents in summary fashion as may be requested by the Covered Entity. The Covered Entity shall not consider as Security Incidents, for the purpose of reporting, external activities (port enumeration, etc.) typically associated with the "footprinting" of a computing environment as long as such activities have only identified but not compromised the logical network perimeter, including but not limited to externally facing firewalls and web servers. The Business Associate shall reasonably use its own vulnerability assessment of damage potential and monitoring to define levels of Security Incidents and responses for Business Associate's operations. However, the Business Associate shall expediently notify the Covered Entity's Privacy Officer of any related Security Incident, immediately upon becoming aware of any unauthorized acquisition including but not limited to use, disclosure, modification, or destruction of PHI by an employee or otherwise authorized user of its system of which it becomes aware.

3.4.1 Business Associate identifies the following key contact persons for all matters relating to this Agreement:

_____
_____
_____
_____
_____
_____
_____

Business Associate shall notify Covered Entity of any change in these key contacts during the term of this Agreement in writing within ten (10) business days.

3.5 Contact for Security Incident Notice. Notification for the purposes of Sections 2.8and 3.4 shall be in writing made by email/fax, certified mail or overnight parcel immediately upon becoming aware of the event, with supplemental notification by facsimile and/or telephone as soon as practicable, to:

TennCare Privacy Officer
310 Great Circle Rd.
Nashville Tennessee 37243
Phone: (615) 507-6697
Facsimile: (615) 734-5289
Email: Privacy.Tenncare@tn.gov

3.6 Security Compliance Review upon Request. Business Associate shall make its internal practices, books, and records, including policies and procedures relating to the security of Electronic PHI received from, created by or received by Business Associate on behalf of Covered Entity, available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's,

Business Associate's compliance with the Security Rule.

3.7 Cooperation in Security Compliance. Business Associate shall fully cooperate in good faith to assist Covered Entity in complying with the requirements of the Security Rule.

3.8 Refraining from intimidation or retaliation. A Covered Entity or Business Associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any Individual or other person for-- (a) Filing of a complaint under 45 C.F.R. § 160.306; (b) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or (c) opposing any act or practice made unlawful, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

4. USES AND DISCLOSURES BY BUSINESS ASSOCIATE

4.1 Use and Disclosure of PHI for Operations on Behalf of Covered Entity. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform Treatment, Payment or Health Care Operations for, or on behalf of, Covered Entity as specified in Service Agreements, provided that such use or disclosure would not violate the Privacy and Security Rule, if done by Covered Entity.

4.2 Other Uses of PHI. Except as otherwise limited in this Agreement, Business Associate may use PHI within its Workforce as required for Business Associate's proper management and administration, not to include Marketing or Commercial Use, or to carry out the legal responsibilities of the Business Associate.

4.3 Third Party Disclosure Confidentiality. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or, if permitted by law, this Agreement, and the Service Agreement, provided that, if Business Associate discloses any PHI to a third party for such a purpose, Business Associate shall enter into a written agreement with such third party requiring the third party to: (a) maintain the confidentiality, integrity, and availability of PHI and not to use or further disclose such information except as required by law or for the purpose for which it was disclosed, and (b) notify Business Associate of any instances in which it becomes aware in which the confidentiality, integrity, and/or availability of the PHI is Breached immediately upon becoming aware.

4.4 Other Uses Strictly Limited. Nothing in this Agreement shall permit the Business Associate to share PHI with Business Associate's affiliates or contractors except for the purposes of the Service Agreement(s) between the Covered Entity and Business Associate(s) identified in the "LIST OF AGREEMENTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT" on page one (1) of this Agreement.

4.5 Covered Entity Authorization for Additional Uses. Any use of PHI or other confidential TennCare information by Business Associate, its Subcontractors, its affiliate or Contractor, other than those purposes of this Agreement, shall require express written authorization by the Covered Entity, and a Business Associate agreement or amendment as necessary. Activities which are prohibited include, but not are not limited to, Marketing or the sharing for Commercial Use or any purpose construed by Covered Entity as Marketing or Commercial use of TennCare enrollee personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws.

4.6 Prohibition of Offshore Disclosure. Nothing in this Agreement shall permit the Business Associate to share, use or disclose PHI in any form via any medium with any third party beyond the boundaries and jurisdiction of the United States without express written authorization from the Covered Entity.

4.7 Prohibition of Other Uses and Disclosures. Business Associate shall not use or disclose PHI that is Genetic Information for underwriting purposes. Moreover, the sale, marketing or the sharing for commercial use or any purpose construed by Covered Entity as the sale, marketing or commercial use of TennCare enrollee personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws, is prohibited.

4.8 Data Use Agreement - Use and Disclosure of Limited Data Set. Business Associate may use and disclose a Limited Data Set that Business Associate creates for Research, public health activity, or Health Care Operations, provided that Business Associate complies with the obligations below. Business Associate may not make such use and disclosure of the Limited Data Set after any cancellation, termination, expiration, or other conclusion of this Agreement.

4.9 Limitation on Permitted Uses and Disclosures. Business Associate will limit the uses and disclosures it makes of the Limited Data Set to the following: Research, public health activity, or Health Care Operations, to the extent such activities are related to covered functions**,** including business planning and development such as conducting cost-management and planning-related analysis related to managing and operating Business Associates functions, formulary development and administration, development and improvement of methods of payment or coverage policies, customer service, including the provision of data analysis for policy holders, plan sponsors, or other customers, to the extent such activities are related to covered functions, provided that PHI is not disclosed and disclosure is not prohibited pursuant to any other provisions in this Agreement related to Marketing or Commercial use.

4.10 Business Associate shall enter into written agreements that are substantially similar to this Business Associate Agreements with any Subcontractor or agent which Business Associate provides access to Protected Health Information.

4.11 Business Associates shall implement and maintain information security policies that comply with the HIPAA Security Rule.

5. OBLIGATIONS OF COVERED ENTITY

5.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of Privacy Practices produced by Covered Entity in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice.

5.2 Notice of Changes in Individual's Access or PHI. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses.

5.3 Notice of Restriction in Individual's Access or PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use of PHI.

5.4 Reciprocity for Requests Received by Business Associate. The Parties agree that this Section (Section 5) is reciprocal to the extent Business Associate is notified or receives an inquiry from any Individual within Covered Entity's covered population.

6. TERM AND TERMINATION

6.1 Term. This Agreement shall be effective as of the date on which it has been signed by both parties and shall terminate when all PHI which has been provided, regardless of form, by Covered Entity to

Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if the Parties agree that it is unfeasible to return or destroy PHI, subsection 6.3.5 below shall apply.

6.2 Termination for Cause. This Agreement authorizes and Business Associate acknowledges and agrees Covered Entity shall have the right to terminate this Agreement and Service Agreement in the event Business Associate fails to comply with, or violates a material provision of this Agreement and any provision of the Privacy and Security Rules.

6.2.1 Upon Covered Entity's knowledge of a Breach by Business Associate, Covered Entity shall either:

(a) Provide notice of breach and an opportunity for Business Associate to reasonably and promptly cure the breach or end the violation, and terminate this BAA if Business Associate does not cure the breach or end the violation within the reasonable time specified by Covered Entity; or

(b) Immediately terminate this BAA if Business Associate has breached a material term of this BAA and cure is not possible.

6.3 Effect of Termination. Upon termination of this Agreement for any reason, except as provided in subsections 6.3.2 and 6.3.5 below, Business Associate shall at its own expense either return and/or destroy all PHI and other confidential information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision applies to all confidential information regardless of form, including but not limited to electronic or paper format. This provision shall also apply to PHI and other confidential information in the possession of sub-contractors or agents of Business Associate.

6.3.1 The Business Associate shall consult with the Covered Entity as necessary to assure an appropriate means of return and/or destruction and shall notify the Covered Entity in writing when such destruction is complete. If information is to be returned, the Parties shall document when all information has been received by the Covered Entity.

6.3.2 This provision (Section 6.3 and its subsections) shall not prohibit the retention of a single separate, archived file of the PHI and other confidential TennCare information by the Business Associate if the method of such archiving reasonably protects the continued privacy and security of such information and the Business Associate obtains written approval at such time from the Covered Entity. Otherwise, neither the Business Associate nor its Subcontractors and agents shall retain copies of TennCare confidential information, including enrollee PHI, except as provided herein in subsection 6.3.5.

6.3.3 The Parties agree to anticipate the return and/or the destruction of PHI and other TennCare confidential information, and understand that removal of the confidential information from Business Associate's information system(s) and premises will be expected in almost all circumstances. The Business Associate shall notify the Covered Entity whether it intends to return and/or destroy the confidential with such additional detail as requested. In the event Business Associate determines that returning or destroying the PHI and other confidential information received by or created for the Covered Entity at the end or other termination of the Service Agreement is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction unfeasible.

6.3.4 Except for Business Associate Agreements in effect prior to April 21, 2005 when the Security Rule became effective, for the renewal or amendment of those same Agreements, or for other unavoidable circumstances, the Parties contemplate that PHI and other confidential information of the Covered Entity shall not be merged or aggregated with data from sources unrelated to that Agreement, or Business Associate's other business data, including for purposes of data backup and disaster recovery, until the parties identify the means of return or destruction of the TennCare data

or other confidential information of the Covered Entity at the conclusion of the Service Agreement, or otherwise make an express alternate agreement consistent with the provisions of Section 6.3 and its subsections.

6.3.5 Upon written mutual agreement of the Parties that return or destruction of PHI is unfeasible and upon express agreement as to the means of continued protection of the data, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction unfeasible, for so long as Business Associate maintains such PHI.

7. MISCELLANEOUS

7.1 Regulatory Reference. A reference in this Agreement to a section in the Privacy and/or Security Rule means the section as in effect or as amended.

7.2 Amendment. The Parties agree to take such action to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191. Business Associate and Covered Entity shall comply with any amendment to the Privacy and Security Rules, the Health Insurance Portability and Accountability Act, Public Law 104-191, and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended, including, but not limited to, changes required by the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

7.3 Survival. The respective rights and obligations of Business Associate under Confidentiality and Section6.3 of this Agreement shall survive the termination or expiration of this Agreement.

7.4 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the Privacy and Security Rules.

7.5 Headings. Paragraph Headings used in this Agreement are for the convenience of the Parties and shall have no legal meaning in the interpretation of the Agreement.

7.6 Notices and Communications. All instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by electronic mail, hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective party at the appropriate facsimile number or address as set forth below, or to such other party, facsimile number, or address as may be hereafter specified by written notice. (For purposes of this section, effective notice to "Respective Party" is not dependent on whether the person named below remains employed by such Party.) The Parties agree to use their best efforts to immediately notify the other Party of changes in address, telephone number, and fax numbers and to promptly supplement this Agreement as necessary with corrected information.

Notifications relative to Sections 2.8 and 3.4 of this Agreement must also be reported to the Privacy Officer pursuant to Section 3.5.

COVERED ENTITY:
Stephen Smith, Director
Division of TennCare
310 Great Circle Rd.
Nashville, TN 37243
Fax: (615) 253-5607

BUSINESS ASSOCIATE:
Craig E. Haseltine, VP
IBM Corporation
6710 Rockledge Drive
Bethesda, MD 20817

All instructions, notices, consents, demands, or other communications shall be considered effectively given as of the date of hand delivery; as of the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing; or on the day the facsimile transmission is received mechanically by the facsimile machine at the receiving location and receipt is verbally confirmed by the sender.

7.7 Transmission of PHI or Other Confidential Information. Regardless of the transmittal methods permitted above, Covered Entity and Business Associate agree that all deliverables set forth in this Agreement that are required to be in the form of data transfers shall be transmitted between Covered Entity and Business Associate via the data transfer method specified in advance by Covered Entity. This may include, but shall not be limited to, transfer through Covered Entity's SFTP system. Failure by the Business Associate to transmit such deliverables in the manner specified by Covered Entity may, at the option of the Covered Entity, result in liquidated damages if and as set forth in one (1) or more of the Service Agreements between Covered Entity and Business Associate listed above. All such deliverables shall be considered effectively submitted upon receipt or recipient confirmation as may be required.

7.8 Strict Compliance. No failure by any Party to insist upon strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement.

7.9 Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.

7.10 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that Tennessee law has been pre-empted by HIPAA and HITECH and without giving effect to principles of conflicts of law. Jurisdiction shall be Davidson County, Nashville, Tennessee, for purposes of any litigation resulting from disagreements of the parties for purpose of this Agreement and the Service Agreement (s).

7.11 Compensation. There shall be no remuneration for performance under this Agreement except as specifically provided by, in, and through, existing administrative requirements of Tennessee State government and Services Agreement(s) referenced herein.

7.12 Validity of Execution. Unless otherwise agreed, the parties may conduct the execution of this Business Associate Agreement transaction by electronic means. The parties may agree that an electronic record of the Agreement containing an Electronic Signature is valid as an executed Agreement.

IN WITNESS WHEREOF, the Parties execute this Agreement to be valid and enforceable from the last date set out below:

DIVISION OF TENNCARE	**BUSINESS ASSOCIATE**
By: Stephen M. Smith Digitally signed by Stephen M. Smith Date: 2022.07.28 09:49:34 -05'00'	By: Craig E Haseltine
Stephen Smith, Director	Craig E. Haseltine, VP
Date:	Date: 6/3/2022

Division of TennCare
310 Great Circle Road
Nashville, TN 37243
Fax: (615) 253-5607

IBM Corporation
6710 Rockledge Drive
Bethesda, MD 20817