



CONTRACT AMENDMENT COVER SHEET

Agency Tracking # 31865-00635	Edison ID 80732	Contract # 80732	Amendment # 1		
Contractor Legal Entity Name Aunt Bertha, A Public Benefit Corporation d.b.a. findhelp			Edison Vendor ID 0000250024		
Amendment Purpose & Effect(s) Language Change, Maximum Liability Increase, Term Extension					
Amendment Changes Contract End Date: ☒ YES ☐ NO		End Date: September 30, 2031			
TOTAL Contract Amount INCREASE or DECREASE per this Amendment (zero if N/A): \$12,126,900.00					
Funding —					
FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2024	\$21,825.00	\$196,425.00			\$218,250.00
2025	\$232,800.00	\$1,003,950.00			\$1,236,750.00
2026	\$467,055.00	\$1,584,495.00			\$2,051,550.00
2027	\$611,100.00	\$1,876,950.00		\$1,000,000.00	\$3,488,050.00
2028	\$531,075.00	\$1,593,225.00		\$1,000,000.00	\$3,124,300.00
2029	\$276,450.00	\$829,350.00		\$1,500,000.00	\$2,605,800.00
2030	\$0.00	\$0.00		\$1,750,000.00	\$1,750,000.00
2031	\$0.00	\$0.00		\$1,750,000.00	\$1,750,000.00
2032	\$0.00	\$0.00		\$500,000.00	\$500,000.00
TOTAL:	\$2,140,305.00	\$7,084,395.00	\$	\$7,500,000.00	\$16,724,700.00
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 Digitally signed by: Crystal Allen DN: CN = Crystal Allen email = crystal.g.allen@tn.gov C = US O = TennCare OU = Fiscal Date: 2026.06.02 08:49:40 -05'00'			<i>CPO USE</i>		
Speed Chart (optional)		Account Code (optional)			

**AMENDMENT #1
OF CONTRACT 80732**

This Amendment is made and entered by and between the State of Tennessee, Department of Finance and Administration, Division of TennCare, hereinafter referred to as the "State" and Aunt Bertha, A Public Benefit Corporation d.b.a. findhelp, hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. The following is added as Contract section A.15.

A.15. The Contractor shall perform activities as directed by TennCare and in alignment with Tennessee's Rural Health Transformation (RHT) Program, with emphasis on improving access and quality of care in rural areas. All work will be conducted in partnership with TennCare and is contingent upon the availability of RHT funding. Contractor shall meet all reporting and compliance requirements as defined by TennCare and CMS for the RHT Program. RHT activities shall remain in effect through the applicable RHT funding period and subject to Contract Section D.4. All Contractor obligations are contingent upon the availability and receipt of such RHT appropriations and may be modified, delayed, or terminated at TennCare's discretion in the event of funding changes.

A.15.1 The Contractor shall:

- A.15.1.1 Align with TennCare on the goals of expanding the Closed Loop Referral System, known as Tennessee Community Compass (TNCC), as identified in Tennessee's CMS-approved RHT funding application;
- A.15.1.2 Submit progress reports, fiscal reports, data metrics, and performance documentation as specified by TennCare and CMS
- A.15.1.3 Adhere to all RHT Program reporting protocols, including technical specifications, timelines, and outcome measures
- A.15.1.4 Provide supplemental information as may be requested during Tennessee's RHT Program reviews or CMS evaluations.
- A.15.1.5 Shall support the implementation of the Tennessee Community Compass by onboarding provider organizations located in rural communities, as well as provider organizations that serve rural populations.
- A.15.1.6 Provide technical supports or solutions to additional community-based organizations in rural communities, including those situated in rural communities and those serving rural populations with technology enhancements to support the TNCC workflow.
- A.15.1.7 Ensure coalition functionality is fully available, operational, and embedded for use by other State agencies, enabling appropriate data access for the purpose of evaluating and improving health outcomes by providing relevant data that are accessible to TennCare for evaluating and improving health outcomes, consistent with TennCare's guidance and applicable laws and policies.
- A.15.1.8 Ensure that coalition functionality is fully available, operational, and embedded for use by partners by providing relevant data that are accessible to TennCare for evaluating and improving health outcomes, consistent with TennCare's guidance and applicable laws and policies.
- A.15.1.9 Conduct community engagement efforts including, but not limited to, onboarding and training, list processing, and partner support ensuring that rural populations

and communities have meaningful access to community-based resources that address identified needs.

- A.15.1.10 Support new technology and enhancements for TennCare's health related social needs strategy.
- A.15.1.11 Provide data enhancements, data analytic support, and improve dashboarding capabilities that directly support TennCare's evaluation of the TNCC, broader impact of TNCC on health outcomes, and in support of support RHT goals.
- A.15.2 The Contractor shall work with TennCare to identify mutually agreed upon requirements, deliverables, and workplans to advance the RHT Program funding goals for each RHT Program year.
 - A.15.2.1 Upon TennCare request, the Contractor shall provide an annual implementation schedule, project schedule, project workplan, or other workplan documentation for TennCare review and approval. Any requested documents will be provided at least sixty (60) calendar days prior to the start of each RHT Program year, unless otherwise directed by TennCare.
 - A.15.2.2 The Contractor shall work with TennCare on mutually agreeable templates for all required documents needed to provide requested deliverables or project documents.
 - A.15.2.3 Contractor shall provide a comprehensive annual report to TennCare after the RHT funding budget period 1 has been approved and issued by CMS. The report shall include, but limited to, the following:
 - a. Strategic goals for strengthening rural networks and provider participation
 - b. Expected impact on rural communities including TennCare members, providers, and community partners
 - c. Assessment of existing rural resource availability within the Findhelp network
 - d. Onboarding strategy and training supports for Community-Based Organizations with rural focus or rural service areas
 - e. Performance and evaluation plan to assess progress over the course of the RHT Program

2. Contract section B.1. is deleted in its entirety and replaced with the following:

- B.1. This Contract shall be effective on December 1, 2023 ("Effective Date") and extend for a period of Ninety-four (94) 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.

3. Contract section B.2. is deleted in its entirety and RESERVED.

- B.2. RESERVED.

4. Contract section C.1. is deleted in its entirety and replaced with the following:

- C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed Sixteen Million, Seven hundred twenty-four thousand, seven hundred dollars (\$16,724,700.00) ("Maximum Liability"). The Maximum Liability shall include the Total Cost of DDI and O&M for the Term, Special Projects and Enhancements, and Authorized User subscription costs. 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.

5. Contract section C.2. is deleted in its entirety and replaced with the following:

- 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.9.1.9. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - b) Data storage tools, capacity, and cost as required by A.9.1.10. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - c) Archiving tools, capacity, and cost as required by A.9.1.11. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - d) Data restore tools, capacity, and cost as required by A.9.1.12. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - e) Cloud services as required by A.9.1.13. shall be included in the Maximum Liability and shall not result in additional cost to State of Tennessee or TennCare.
 - f) All costs associated with the facility as required by A.12.4. 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
 - g) All goods or Services, as applicable to the Solution, to satisfy the requirements in Sections A.3. through A.15. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.

Notwithstanding the above, TennCare may, in its sole discretion, utilize alternative purchasing methods for purchases under this Contract, in whole or in part,. In the event that TennCare utilizes alternative purchasing methods, in whole or in part, for any goods or services proposed by the Contractor, such costs as detailed in Attachment G, Schedule G shall be reduced from the Total Cost for DDI and O&M and Maximum Liability through an Amendment in accordance with D.3.

6. The Contract section C.3. is deleted in its entirety and replaced with the following:

- 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 shall include all Deliverables and other activities required in the TennCare Solution Implementation Lifecycle. The standard method for Payment under this Contract to the 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 CLRS Solution.
 - 2) 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.

- 3) 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 Phase Cost as described in this Section.
- 4) 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 CM 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.
- 5) 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.
- 6) The alteration to the Payment and withhold structure shall be deemed to be made at the time that TennCare notifies the Contractor in writing.
- 7) 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:

DDI Phase I	Gate Reviews	Gate Review Milestone Payment %	Gate Review Milestone Payments
Planning	Project Baseline Review	10%	\$ 72,750.00
Requirements Review	Requirements Review	20%	\$ 145,500.00
Design	Final Detailed Design Review	5%	\$ 36,375.00
Development	Validation Readiness Review	7%	\$ 50,925.00
Test	Implementation Readiness Review	8%	\$ 58,200.00
Issuance of State Acceptance Letter		20%	\$ 145,500.00
DDI Phase II	Gate Reviews	Gate Review Milestone Payment %	Gate Review Milestone Payments
Requirements Review	Requirements Review	4%	\$ 29,100.00
Design	Final Detailed Design Review	4%	\$ 29,100.00
Development	Validation Readiness Review	6%	\$ 43,650.00
Test	Implementation Readiness Review	6%	\$ 43,650.00

DDI Phase I	Gate Reviews	Gate Review Milestone Payment %	Gate Review Milestone Payments
Additional Reviews		Additional Milestone Payment %	Additional Milestone Payments
Completion of Warranty		10%	\$ 72,750.00
Phased O&M		Annual Cost	
O&M Phase 1		\$ 582,000.00	
Solution O&M		Annual Cost	
Solution O&M		\$ 582,000.00	

The Contractor shall be compensated for Authorized User fees based upon the actual number of Authorized Users for the previous calendar month during the O&M Phase based on the payment methodology listed below.

The following Authorized Users tiers are effective through November 30, 2028:

Authorized Users	Monthly Cost
Unlimited (> 3001 Authorized Users)	\$ 97,000.00
Authorized Users Tier	Monthly Cost per Tier
Tier 1: 1-750 Authorized Users	\$ 77,600.00
Tier 2: 751-1500 Authorized Users	\$ 58,200.00
Tier 3: 1501-2550 Authorized Users	\$ 38,800.00
Tier 4: 2251-3000 Authorized Users	\$ 19,400.00

The following authorized Users Tier is effective through December 1, 2028 through the end of the RHT Funding period, September 30, 2031.

Authorized Users	Monthly Cost
Unlimited (> 3001 Authorized Users)	\$ 97,000.00
Authorized Users Tier	Monthly Cost per Tier
Tier 1: 1-750 Authorized Users	\$ 19,400.00
Tier 2: 751-1500 Authorized Users	\$ 38,800.00
Tier 3: 1501-2550 Authorized Users	\$ 58,200.00
Tier 4: 2251-3000 Authorized Users	\$ 77,600.00

- c) The Contractor shall be compensated for Special Project Change Orders and Enhancement Change Orders requested and performed pursuant to Contract Section A.12.6. 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, PROVIDED THAT:
 - 1) Compensation to the Contractor for Special Project Change Orders shall not exceed ten percent (10%) 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 ten percent (10%) 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) 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	\$ 189,150.00 (10% of the Total DDI and O&M Costs)
Enhancement Change Order Request	\$ 189,150.00 (10% of the Total DDI and O&M Costs)

C.3.d. The Contractor shall be compensated upon the satisfactory provision of goods or services as described in Contract Section A.15. All compensation is subject to and contingent upon federal approval for RHT funding and Contract Section D.4. Eligible compensation is based upon the following payment methodology:

Based on state and federal guidance and contingent on approval for additional federal budget periods by CMS, TennCare will establish a detailed individual payment schedule, not to exceed the RHT Program annual funding listed in Section C.3.d.1., and TennCare will provide the Contractor instructions, additional information, accounting, and invoicing requirements in accordance with Contract Section A.12.7. or Contract Section E.4., as applicable.

1)

RHT Budget Period	Anticipated Funding (Final Funding Amount to be Approved by CMS)
Budget Period 1	\$500,000.00
Budget Period 2	\$500,000.00
Budget Period 3	\$2,000,000.00
Budget Period 4	\$2,000,000.00
Budget Period 5	\$2,500,000.00
Total Funding	\$7,500,000.00

- 2) Unless otherwise directed by TennCare, RHT Funding will be distributed as specified in Sections C.3. with the following additional requirements including:
 - a. RHT O&M Annual Cost for all remaining contract years shall not exceed an annual amount of Five Hundred Eighty-Two Thousand Dollars (\$582,000).
 - b. Contractor shall be compensated for any new RHT Special Project Change Orders, Enhancement Change Orders, or deliverables requested and performed pursuant to Contract Section A.15 or otherwise directed by TennCare for the purposes of supporting A.15 without a formal amendment of this Contract. Total compensation for these activities will not exceed the total amount of approved and allocated funding through RHT Program. RHT Special Project Change Order Requests and Enhancement Change Order Requests to support project requirements and

reimbursed through approved RHT funds will not be counted for the purposes of the ten percent (10%) of the total Closed Loop Referral System DDI and O&M cost limit.

- c. The Contractor shall be compensated for Authorized User fees based upon the actual number of Authorized Users for the previous calendar month during the O&M Phase based on and up to the annual cost allocated for RHT Program.

7. Contract Section E.20 is deleted in its entirety and replaced with the following:

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 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 twenty-four (24) 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. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. 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.

8. Contract Section E.26 is deleted in its entirety and replaced with the following:

E.24. 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 twenty-four (24) 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, and/or disks

9. **Contract Attachment A is deleted in its entirety and replaced with new Attachment A.**

10. **Contract Attachment F is deleted in its entirety and replaced with new Attachment F.**

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective once all required approvals are obtained. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

IN WITNESS WHEREOF,

AUNT BERTHA, A PUBLIC BENEFIT CORPORATION D.B.A. FINDHELP:

Erine Gray

05/26/2026

254356C9F99592C77D22E840DBA367C8

contractworks.

SIGNATURE

DATE

Erine Gray - President & CEO

PRINTED NAME AND TITLE OF SIGNATORY (above)

**DEPARTMENT OF FINANCE AND ADMINISTRATION
DIVISION OF TennCare:**

Jim Bryson / JB

5/26/2026

JIM BRYSON, COMMISSIONER

DATE

ATTACHMENT A - DEFINITIONS AND ABBREVIATIONS

For the purposes of the Closed-Loop Referral System (CLRS) Request for Proposal (RFP) and resulting Contract, the following definitions of terms shall apply, unless otherwise indicated. All Deliverables not defined here shall be as defined in the TennCare Solution Implementation Lifecycle RACI and Deliverables document, included in the Procurement Library and Table 4: Table of Deliverables in the Contract.

1.1 Definitions

Term	Definition
Acceptance	A notice from TennCare to the Contractor that a Deliverable or Service has conformed to its applicable acceptance criteria in accordance with the process described in the TennCare Solution Implementation Lifecycle (SILC) RACI and Deliverables.
Acceptable Use Policy	A set of rules and guidelines meant to govern an employee's use of a company's technology resources, including the internet. When implemented at a company, an AUP clearly communicates what is (and is not) permitted on company computers and networks.
Access Controls	A security technique that dictates who or what is allowed to view or use system resources.
Accessibility	Electronic and information technology (EIT) designed to work for all people, whatever their hardware, software, browser source, language, culture, location, or physical or mental ability. When EIT meets this goal, it is accessible to people with a diverse range of hearing, movement, sight, and cognitive ability. For reference please visit: https://www.w3.org/standards/webdesign/accessibility
Active Community-Based Organization (CBO) Service Location	A Verified CBO Service Location where an Authorized User associated with that CBO Service Location logs into the Solution at least weekly.
Advanced Persistent Threat (APT)	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Artifacts	Documents created by the project to describe the Solution or service being implemented and the processes used to define, implement, and manage the Solution.
Assessor	A qualified, third-party, independent audit firm, approved by TennCare, to conduct an assessment of the security and privacy controls in the Solution and maintain the integrity of the audit process.

Authorized User	An individual that has specified access rights to a given area, system, or sub-system. Authorized Users may include Providers, Managed Care Organizations (MCOs), Community-Based Organizations (CBOs), and TennCare.
Business Days	Monday through Friday from 8:00 AM – 5:00 PM Central Standard Time (CST); TennCare holidays are excluded. A list of TennCare Holidays can be located at https://www.tn.gov/about-tn/state-holidays.html
Care Coordination Tool (CCT) Contractor	The contractor operating the Solution in support of TennCare's Care Coordination Tool (CCT) that provides claims, clinical, and Member-attributed data to Authorized Users.
Centers for Medicare and Medicaid Services (CMS)	The organizational unit of the U.S. Department of Health and Human Services responsible for administration of the Title XIX and Title XXI Programs under the Social Security Act.
Certification Crosswalk	Documentation that the Contractor needs to provide on how the outcomes-based Key Performance Indicators (KPIs) are met, such that TennCare can sufficiently adhere to the required CMS Certification guidelines and criteria.
Change Management	The process of identifying and implementing changes within a system.
Change Order	A written form, in response to a Change Request that is mutually agreed upon by TennCare and the Contractor, which modifies, deletes, or adds to the deliverables or services, in whole or in part, and that is made in accordance with the Change Order terms.
Change Request	A written form used to propose that the deliverables or services be modified, deleted, or added to, in whole or in part, made in accordance with the change request terms.
Children's Health Insurance Program (CHIP)	Authorized under Title XXI of the Social Security Act. CHIP provides low-cost health coverage to children in families whose incomes exceed the standard limits to qualify for Medicaid. Tennessee's CHIP is referred to as CoverKids.
Closed-Loop Referral System or Solution	Contractor-provided cloud-native SaaS Solution utilized for non-medical needs assessment, community resource directory purposes, community resource identification, non-medical risk factors referral system, and closed-loop referrals. The TennCare-specific system is known as Tennessee Community Compass (TNCC).
Cloud Service Provider (CSP)	A third-party company that offers components of cloud computing, including a cloud-based platform, infrastructure, application, or storage services.
Cloud Solution	A solution that fully utilizes commercially available Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS) components. Solutions that leverage infrastructure provided by the Contractor are not considered cloud solutions. Cloud native capabilities include, but are not limited to, dynamic CPU allocation, auto-scaling, loosely coupled micro services, and containerization. Cloud-based environments within the Medicaid Modernization Program (MMP) must be compliant with the Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
CMS Certification	The CMS-written acknowledgement that the Closed-Loop Referral System (CLRS) meets all legal and operational requirements necessary for Enhanced Federal Financial Participation (EFTP) as outlined within the criteria and guidelines set forth by CMS.
Commercial off-the-shelf (COTS)	A software that is ready to use without any modification by the user and is available from commercial sources. Examples of COTS software include, but are not limited to, SaaS, and commercially available cloud-based services and solutions, such as Amazon Web Services (AWS).

Community-Based Organization (CBO)	A public or private organization which provides mission-driven support services to individuals in the community.
Community-Based Organization (CBO) Service Location	A physical address of a CBO where services can be accessed, information can be acquired about services offered, and/or the staff of the organization are housed. If a CBO has one or more location, regardless of the distance between locations, each location shall be counted as unique for the purposes of any Performance Metric Payment (i.e., three CBO Service Locations are counted three times). While a CBO may have locations across multiple states, only locations within Tennessee should be counted. If a CBO does not have a physical location in Tennessee (e.g., CBO operates two locations in northwest Mississippi that are active and confirmed for community-based services as part of the TennCare Health Starts Initiative), the out-of-state locations will should only be counted once for the purposes of any Performance Metric Payment.
Community Resource Directory	A resource directory which contains non-medical service providers and services (e.g., CBOs) available to address Non-Medical Risk Factors. The Community Resource Directory will contain validated and updated organization, program, and service-level contact information.
Confidential Information	Any non-public, confidential, or proprietary information, whether written, graphic, oral, electronic, visual, or fixed in any tangible medium or expression, supplied by TennCare. This includes individuals enrolled in any TennCare program or relating to individuals who may be potentially enrolled in a TennCare program, to the extent that confidential status is afforded such information under State and/or Federal laws or regulations. All confidential information shall not be subject to disclosure under the Tennessee Public Records Act.
Configuration Management	The process of documenting formal procedures to apply technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a product, result, service, or component; control any changes to such characteristics; record and report each change and its implementation status; and support the audit of the products, results or components to verify conformance to requirements. It includes the documentation, tracking systems, and defined approvals necessary for authorizing and controlling changes. Configuration Management Controls include, but are not limited to: — CM-2: Detailed configuration settings consistent with CM-2 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations. — CM-6: Detailed configuration settings consistent with CM-6 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations. — CM-8: Equipment listing consistent with CM-8 (Configuration Management as per NIST 800-53) that supports the system/application.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT service.
Continuous Improvement Process (CIP)	The process of aligning an organization's services and processes with changing business needs through the ongoing identification and improvement of elements involved in the management of products, processes, and services.

Contractor	The entity performing services pursuant to this Contract, including any officer, owner, member, director, employee, volunteer, agent, subcontractor, representative, and/or assignee of the Contractor, and any other person, partnership, corporation, or other legal entity performing work or services, or providing materials, under this Contract for or on behalf of the Contractor. For purposes of any permitted subcontract, "Contractor" includes any subcontractor(s), owners, members, officers, directors, partners, employees, and/or agents.
Dashboard	A visual representation of the results of a query run on data. A dashboard brings together useful information on a series of screens and/or web pages. Information contained in a dashboard includes, but is not limited, to reports, web links, calendar, news, tasks, and e-mail.
Data Ecosystem (DE) Contractor(s)	The contractor(s) providing the Data Ecosystem components that collectively make up the TennCare Data Ecosystem Solution. Data Ecosystem components include the Enterprise Data Warehouse (EDW), Data Quality/Extract- Transform-Load (DQ/ETL) Pipeline, Master Data Management (MDM), and the Decision Support System (DSS).
Data Governance	A set of internal policies and procedures to align the organization with the business strategy, enable prioritization and approval of initiatives, and a plan for the introduction of processes which will continuously monitor and improve data quality.
Data Mining	The process of examining large data stores to identify patterns or extract usable data.
Data Model	A framework for the development of new or enhanced application(s) for development of an accurate model or graphical representation of information needs and business process.
Data Quality	A measure of the condition of data based on factors such as accuracy, completeness, consistency, and reliability.
Data Set	A collection of individual but related items of data that can be accessed and processed as individual items or collectively.
Data Source	Also referred to as "source system" is the database from which a specific piece of data originated.
Database	A collection of information stored in an organized, structured manner for fast and convenient search and retrieval by business applications and Business Intelligence software.
Defect	Any nonconformance of the goods or services to the terms and conditions of the Contract. A Defect may include issues that occur with the Solution at the component or sub-system level and may lead to a failure (deeming the Solution "Defective"). A Defect can exist within testing and production environments, resulting in non-conformance of the design and/or requirements associated with the Solution.
Deliverables	All services, tangible and intangible products TennCare intends the Contractor to produce, prepare, and deliver during the course of the Contractor's performance under this Contract, including those described in the Contract and the TennCare Solution Implementation Lifecycle RACI and Deliverables.
Design, Develop, and Implement (DDI)	The phases encompassing the Solution design, development activities, and implementation of required business and technical functionality.

Disaster	An unplanned interruption of the IT infrastructure components used to support business process. Disasters include, but are not limited, to the following: bomb threat, civil disturbance, cyber incident, earthquake, internal fire, external fire, internal flood, external flood, generator failure, hazmat exposure, ice event, pandemic, power outage, prolonged IT outage, severe thunderstorm, temperature extremes, tornado, workplace violence, and/or utility failure (e.g., HVAC, water, gas).
Domain	A group of Non-Medical Risk Factors defined by HHS and utilized by Healthy People 2030 to create a place-based framework. The five domains Healthy People 2030 defined are the following: 1. Economic Stability – The connection between the financial resources people have - income, cost of living, and socioeconomic status - and their health. This area includes key issues such as poverty, employment, food security, and housing stability. 2. Education Access and Quality – The connection of education to health and wellbeing. This domain includes key issues such as graduating from high school, enrollment in higher education, educational attainment in general, language and literacy, early childhood education and development. 3. Healthcare Access and Quality – The connection between people's access to and understanding of health services and their own health. This domain includes key issues such as access to healthcare, access to primary care, health insurance coverage, and health literacy. 4. Neighborhood and Built Environment – The connection between where a person lives - housing, neighborhood, and environment - and their health and wellbeing. This includes topics like quality of housing, access to transportation, availability of healthy foods, air and water quality, and neighborhood crime and violence. 5. Social and Community Context – The connection between characteristics of the contexts within which people live, learn, work, and play, and their health and wellbeing. This includes topics like cohesion within a community, civic participation, discrimination, conditions in the workplace, and incarceration. A list of Healthy People 2030 Domains can be found at: https://health.gov/healthypeople/objectives-and-data/social-determinants-health
Electronic Health Record (EHR)	An electronic version of a Member's medical history, that is maintained by the Provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular Provider, including, but not limited to, demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.
Electronic and Information Technology	Also referred to as Information and Communication Technology (ICT), which means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; web sites; videos; and electronic documents. See 36 C.F.R. Pt. 1194, App. A.

Enterprise-Wide	A term encompassing the entire TennCare organization that is inclusive of all programs and services under the scope of this Contract, rather than a single business department or function.
Event	An event is defined as any Incident that has significance for the management of an IT service or other configuration item.
Event Management	The process that monitors all events that occur through the IT infrastructure, thereby allowing for normal operation and also detecting and escalating exception conditions.
File Integrity Monitoring (FIM)	An internal monitoring solution that validates and detects file changes that could be indicative of a cyber-attack.
Functional Requirement	A requirement that defines specific behaviors or functions the Solution must perform as part of the Contract.
Gate Review	A phase-driven go/no-go decision point where project activities are reviewed to assure that appropriate requirements are observed. A project cannot proceed without a "Go" decision by the appropriate TennCare management for a specific stage gate. Gate Reviews will be conducted in accordance with the processes described in the TennCare Solution Implementation Lifecycle (SILC).
Go-Live	An event when the Solution functionality is deployed and made available in a production environment for operational usage.
Governance, Risk, and Compliance (GRC)	The integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity.
Grand Region	A defined geographical region that includes a distinct list of specified counties for which the Contractor is required to report on separately. The following counties constitute the three Grand Regions in Tennessee: East Grand Region – Anderson, Bledsoe, Blount, Bradley, Campbell, Carter, Claiborne, Cocke, Franklin, Grainger, Greene, Grundy, Hamblen, Hamilton, Hancock, Hawkins, Jefferson, Johnson, Knox, Loudon, Marion, McMinn, Meigs, Monroe, Morgan, Polk, Rhea, Roane, Scott, Sequatchie, Sevier, Sullivan, Unicoi, Union, and Washington Counties. Middle Grand Region – Bedford, Cannon, Cheatham, Clay, Coffee, Cumberland, Davidson, DeKalb, Dickson, Fentress, Giles, Hickman, Houston, Humphreys, Jackson, Lawrence, Lewis, Lincoln, Macon, Marshall, Maury, Montgomery, Moore, Overton, Perry, Pickett, Putnam, Robertson, Rutherford, Smith, Stewart, Sumner, Trousdale, Van Buren, Warren, Wayne, White, Williamson, and Wilson Counties. West Grand Region – Benton, Carroll, Chester, Crockett, Decatur, Dyer, Fayette, Gibson, Hardeman, Hardin, Haywood, Henderson, Henry, Lake, Lauderdale, Madison, McNairy, Obion, Shelby, Tipton, and Weakley Counties.
Graphical User Interface (GUI)	A visual way of interacting with a computer using items such as windows, icons, and menus, which are used by most modern operating systems.
HIPAA Health Insurance Portability and Accountability Act (HIPAA)	The federal law enacted in 1996 which includes requirements to protect patient privacy, security of EHRs, and to prescribe methods and formats for exchange of electronic medical information.
Health Information Technology for Economic and Clinical Health (HITECH)	The federal law enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009 to promote the adoption and meaningful use of health information technology.

Health Starts Initiative	TennCare's approach to addressing Non-Medical Risk Factors in the TennCare population. The Health Starts Initiative implies that health begins outside of the clinical setting and is largely driven by factors that exist in the environments where Members spend the majority of their time. Some of these factors include access to healthy foods, access to adequate and stable housing, transportation access, economic stability and employment opportunities, and social connectedness. These factors play a significant role in an individual's health and quality of life. Unaddressed Non-Medical Risk Factors and their associated needs can lead to poor health outcomes thereby increasing healthcare expenditures for the State. TennCare's goal is for all Members to be screened for these risk factors using a unified approach, for Members to be referred to CBOs to meet identified non-medical needs, and for outcomes to be tracked. This process can be fragmented and often unsuccessful due to varying workflows, differing cultures among stakeholders, technological hinderances, and other challenges. To overcome these challenges and build upon the Health Starts Initiative, TennCare is seeking a statewide Solution that creates connectivity between stakeholders, increases care coordination and support to Members, and streamlines data collection to effectively measure impact - all of which are pillars of TennCare's Health Starts Initiative vision.
Human-Readable	A representation of data or information that can be naturally read by humans without additional tools and software.
Identity and Access Management (IAM)	This component provides the capability to authenticate and authorize users to make use of TennCare's IT services, data, or other assets. The IAM helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify the assets.
Incident Management	The process responsible for managing the lifecycle of all incidents. The purpose of Incident Management is to restore normal service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained.
Industry Standard	A set of criteria within an industry relating to the standard functioning and carrying out of operations in their respective fields of production. It is the generally accepted requirements followed by the members of an industry.
Information Technology Infrastructure Library Version 3.0 (ITIL v3.0)	The third version of the Information Technology Infrastructure Library (ITIL), a globally recognized collection of best practices for IT service management that focuses on aligning IT services with the needs of business.
Information Technology (IT) Operations Management	The administration of technology components and application requirements within TennCare.
Information Technology Service Management (ITSM)	A strategic approach for designing, delivering, managing, and improving the way Information Technology (IT) is used within an organization. The goal of IT Service Management is to ensure that the right processes, people, and technology are in place so that the organization can maximize business value from the use of information technology.
Integration Services (IS) Contractor	The contractor providing the Integration Services Layer (ISL) for the integration and orchestration for all MMIS modules in the MMP. ISL components include, but are not limited to, the Enterprise Service Bus (ESB), Identity and Access Management (IAM), Application Programming Interface (API) Gateway & Proxy, Managed File Transfer (MFT), Electronic Data Interchange (EDI), Enterprise Content Management (ECM), and Service Desk Support.

Key Personnel	The Contractor personnel deemed by TennCare to be essential, from design through implementation, to the Contractor's satisfactory performance of the requirements contained in the Contract as described in the Key Personnel Table in A.12.3.
Knowledge Management	The process of identifying, organizing, storing, and disseminating information within an organization.
Limited English Proficient (LEP)	Individuals who do not speak English as their primary language and who have a limited ability to read, write, speak, or understand English and may be eligible to receive language assistance with respect to a particular type of service, benefit, or encounter.
Liquidated Damages (LDs)	A clause that specifies a predetermined amount of money that must be paid as damages for failure to perform under the Contract.
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.
Master Data Management (MDM)	The MDM component of the Data Ecosystem solution that provides the framework, tools, and processes to ensure that data is consistently defined, linked, and managed throughout the enterprise. The MDM shall utilize a consistent methodology for the management of Enterprise-Wide data aligned with the TennCare Data Governance structure.
Medicaid	The Federal medical assistance program authorized in Title XIX of the Social Security Act, administered by States and U.S. Territories.
Medicaid Information Technology Architecture (MITA)	An initiative by CMS to foster integrated business and IT transformation across the Medicaid enterprise to improve the administration of the Medicaid program. It promotes modernization of MMIS operations through modular frameworks with greater interoperability among systems or solutions, use of COTS software, reusable programs and systems, and system analysis which allows business needs to drive system development.
Medicaid Management Information System (MMIS)	The MMIS is a mechanized claims processing and information retrieval system that State Medicaid programs must have to be eligible for Federal funding. For Title XIX purposes, "systems mechanization" and "mechanized claims processing and information retrieval systems" is identified in section 1903(a)(3) of the Act and defined in regulation at 42 CFR 433.111. The objectives of this system and its enhancements include the Title XIX program control and administrative costs; service to recipients, Providers, and inquiries; operations of claims control and computer capabilities; and management reporting for planning and control.
Medicaid Management Information System (MMIS) Modules	A collection of MMIS business functionality and processes that can be implemented through a variety of IT capabilities and services. The MMIS modular structure provides scalability to TennCare programs, by enabling the flexibility of integrating new components at a lower risk and cost, as programs and technologies evolve. MMIS Modules include, but are not limited to, Integration Services (IS), Data Ecosystem (DE), Provider Services, Pharmacy Benefit Management (PBM), Dental Benefits Management (DBM), Tennessee Eligibility Determination System (TEDS), Financial Management, Encounter Processing, and other core and ancillary TennCare applications and systems.
Medicaid Modernization Program (MMP)	MMP is an all-encompassing term used to describe TennCare's various initiatives and projects aimed at streamlining its Medicaid program to improve operational efficiencies and service delivery through industry-leading enabling technologies.

Medicaid Modernization Program Vendors and Partners (MMPVP)	Medicaid Modernization Program Vendors and Partners (MMPVP) include, but are not limited to, the following TennCare vendors and partners: — Technical Advisory Services (TAS): TAS supports and advises TennCare in completing the TennCare Information Services Portfolio by offering organizational change management and training, operations & maintenance planning, lifecycle advisory services, quality management, and enterprise architecture services. — Strategic Program Management Office (SPMO): The SPMO provides program and project management support to TennCare IS. — MMIS Module Vendor(s): The modular vendor partners who design, implement, test, and maintain the systems, applications, and business and technology services that support the enterprise. MMIS modules use the ISL to consume or provide services or data across solutions and modules throughout the TennCare enterprise. — Business Support Services (BSS): Assists with strategic planning and development of business enterprise architecture strategy, providing subject-matter expertise supporting certification, testing, MITA, and Advanced Planning Documents (APD). BSS assists TennCare in preparing for and coordinating project reviews, including documentation of existing processes and recommendations for future process improvements.
Member	An individual who has healthcare coverage through a program administered by TennCare.
Metadata	Data that describes and gives information about other data, including a structured description of data characteristics reflecting the meaning, content, structure, usage, and purpose of a data object.
Minimum Accept Risk Standards for Exchanges (MARS-E)	A document suite of guidance, requirements, and templates assembled by CMS. The document suite contains implementation standards for key security requirements contained in Department of Health and Human Services (HHS) Affordable Care Act (ACA) Regulations (45 CFR §§155.260 and 155.280) and other State and Federal regulations and policies. This is a harmonized set of guidelines inclusive of CMS and IRS requirements. Any reference to this package, even under CMS context references, should also infer compliance with current IRS Safeguards Program and IRS Pub 1075, where applicable by usage of data type and/or classification.
Module Support Team	A support team staffed for the Solution for the purpose of resolving Incidents that are directly related and applicable to the Solution's performance. Module Support consists of resources with technical expertise related to the Solution and should include Tier – II and III Level support capabilities. Once the Contractor resolves the Incident, the Contractor is responsible for reporting the resolution results to the Tier I – Service Desk level.
Multi-Factor Authentication (MFA)	An authentication method that requires users attempting to log-in to a resource to provide two or more factors of verification to gain access.
Network Operations Center (NOC)	A centralized location where TennCare's IT team can continuously monitor the performance and health of a network.
Non-Authenticated User	An individual that only has privileges to the public-facing Community Resource Directory to conduct searches on specified criteria related to social service domains. Non-Authenticated Users can include Members, or any other user not included as Authorized Users.
Non-Functional Requirement	A requirement that specifies criteria that can be used to validate the operation of the Solution, rather than specific Solution behaviors. Non-Functional requirements evaluate if the Solution is "fit for use."

Non-Medical Needs Assessment	A process of gathering information to identify health-related non-medical needs. The Non-Medical Needs Assessment is used to identify Domains for the Referral, if applicable.
Non-Medical Risk Factor	A factor in a Member's life outside of traditional medical care that contributes to the risks and resiliency of the Member's health and quality of life. Non-Medical Risk Factors can include economic instability, lack of education access, healthcare access, neighborhood and built environment, and social and community context.
On-demand	On-demand shall mean making data available to an Authorized User as needed to support the Solution capability the Authorized User is invoking.
On-Site	On-Site shall mean that the Contractor staff and/or subcontractors shall be physically present at any of the TennCare designated offices, the Contractor's offices located in Nashville, Tennessee, or as otherwise approved by TennCare. On-Site positions require the Contractor staff and/or subcontractors to meet the dedication requirements for each role. On-Site may include virtual presence at the direction or discretion of TennCare.
Operational Readiness Review (ORR)	A review to ensure that the Solution is being implemented into production and is ready for Go-Live. System readiness, organizational change management, and outreach activities are also verified.
Operational Readiness Test (ORT)	A technical testing activity to ensure that a module, integrated with other modules, complies with Non-Functional Requirements.
Operations & Maintenance (O&M) Phase	Maintenance and support services that will be performed by a Contractor to improve performance or other attributes associated with the Solution.
Operations & Maintenance (O&M) Cost	Total cost of maintenance and support services that will be performed by a Contractor in O&M Phase 1 and Solution O&M to improve performance or other attributes associated with the Solution.
Patient-Centered Medical Home (PCMH)	A PCMH is a model of care that strengthens the clinical-patient relationship by replacing episodic care with coordinated, whole person, and long-term care. The primary care clinician leads a team of clinical and community health providers who take collective responsibility for patient care. They coordinate care for the patient's health needs and arrange for appropriate care with other qualified health services. This definition can be found on the CDC's website at: https://www.cdc.gov/nccdphp/dch/pdfs/dch-cmh-issue-brief.pdf
Payment	The amount(s) to be paid for Deliverables and Services provided under this Contract, in whole or in part, as described in the Cost Proposal of the Contract and Section C of the Contract, and any subsequent written amendments or Change Orders.
Problem	A cause, or potential cause, of one or more Incident(s) and associated Defect(s) classification(s). Problem(s) can be raised in response to a single significant Incident and assigned Defect classification (Critical, High, Medium, or Low) or multiple similar Incidents and assigned Defects (regardless of classification level). Problem(s) can also be raised without the existence of a corresponding incident, where a Defect categorization has solely been assigned (e.g., bug-fixing).
Performance Metric Payment	A risk-based, performance-based payment representing Pass/Fail criteria established by TennCare. The performance period represents a defined three-month period, with payment or penalty assessment to be applied to the O&M Monthly Cost for the month immediately preceding the end of the quarterly performance period.

Problem Management	The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the impact of Incidents that cannot be prevented.
Processes	Structured set of activities designed to accomplish a specific objective turning inputs into defined outputs. It may include roles, responsibilities, tools, and management controls required to deliver outputs.
Provider	A TennCare-registered healthcare professional licensed, authorized, certified, or regulated under T.C.A. Title 63 Professions of the Healing Arts with a valid TennCare/Medicaid ID number.
Quality Management Standards	The mandatory requirements for a product, service, or process to align in order to provide the intended value expressed by TennCare.
Referral	A tool to facilitate access to community-based resources to address unmet Non-Medical Risk Factors. Referral capabilities include: — The ability to send Member Referrals via the CLRS to CBOs or other TennCare service partners (e.g., MCOs). — The ability to receive information back from the CBOs or designated TennCare service partners via the CLRS to Authorized Users about outcomes of the Referral.
Release and Deployment Management	The process responsible for both release management and deployment management. Release management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. The primary objective of release management is to ensure that the integrity of the live environment is protected and that the correct components are released. Deployment management is the activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment.
Request Fulfillment	The process responsible for managing the lifecycle of all service requests from Authorized Users.
Rural Health Transformation (RHT) Program	A five-year federal initiative, in which the State of Tennessee received federal appropriation, that focuses on improving healthcare challenges in rural areas. The federal appropriation was authorized by the Tennessee General Assembly (Section 71401 of Public Law 119-21) which includes initiatives specific to TennCare.
Software as a Service (SaaS)	A software licensing and delivery model in which software is licensed for use on a subscription basis and is cloud hosted. Instead of installing and maintaining software, TennCare will simply access it via the Internet, freeing itself from software and hardware management.
Sensitive Data	Any data or record that identifies a person, including health information or financial information, and any data or record designated as sensitive, proprietary, or confidential by TennCare, State, or Federal law or regulation. Examples of Sensitive Data include, but is not limited to, Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), Protected Health Information (PHI), Social Security Administration (SSA), Criminal Justice Information Services (CJIS), Tennessee Bureau of Investigation (TBI), and Federal Tax Information (FTI).
Service	Any and all services, Deliverables, materials, Special Project Change Orders, Enhancement Change Orders, and any other work requirement to be performed by the Contractor pursuant to the Contract.
Service Asset	Any resource or capability of a service provider.
Service Catalog	Structured information about all the services and service offerings of a service provider, relevant for a specific target audience.

Service Design	An ITIL service lifecycle stage encompassing the design of new services, as well as changes and improvements to existing services, that are fit for purpose, fit for use, and that can be delivered by the organization and its ecosystem.
Service Desk	The single point of contact between the Contractor and the Authorized Users. A typical Service Desk manages incidents and service requests and handles communication with the Authorized Users.
Service Level Agreement (SLA)	An instrument to measure performance expectations between TennCare and the Contractor that detail the characteristics, quality, delivery standards, timeframe, and/or scope of Services to be provided.
Service Lifecycle	An approach to IT Service Management (ITSM) that emphasizes the importance of coordination and control across the various functions, processes, and systems necessary to manage the full lifecycle of IT services.
Service Portfolio	A complete set of products and services that are managed throughout their lifecycles by an organization.
Service Strategy	An ITIL service lifecycle approach to understand the service offerings required to meet TennCare's business/operational needs, supporting IT capabilities and resources that are required to develop these offerings, and the requirements to execute these service offerings.
Service Transition	The process that ensures new, modified, or retired services meet the expectations of the business as documented in the service strategy and service design stages of the IT lifecycle.
Service-Oriented Architecture (SOA)	A software design strategy that packages common functionality and capabilities (services) with standard, well-defined service interface to produce formally described functionality invoked using a published service contract.
Severity Level 1 Incident	The incident severity level ranking representing that the Solution, or any business-critical function, is unusable or unavailable for multiple end-users; there is no available workaround.
Severity Level 2 Incident	The incident severity level ranking representing that the ability to use the Solution, or any business-critical function, is severely limited. The Contractor and TennCare will agree upon what is "severely limited" prior to assigning the priority level to the incident; there is an acceptable workaround for the issue.
Severity Level 3 Incident	The incident severity level ranking representing that the Solution, or any business-critical function is useable, but there is some degradation of a normally provided function. Impact on end-users is significant but not disabling or severe; there is an easy workaround to the issue.
Severity Level 4 Incident	The incident severity level ranking representing that the Solution or business critical function is usable, but the issue is apparent. Impact on end-users is considered minimal (generally these issues are cosmetic in nature).
Solution	The Contractor-proposed Solution shall support the requirements within the Contract and include all costs and configurations for hardware, software, cloud, and infrastructure required to acquire, install, operate, and maintain the CLRS.
Subject Matter Professional	A stakeholder with in-depth knowledge of a topic relevant to the business need or solution scope.
Stakeholder	A Stakeholder refers to state and federal government agencies, TennCare MCOs, health information organizations throughout the State, Members, families, provider associations, medical professionals, medical and school communities, CBOs, interest groups, or any other partners TennCare deems appropriate.
Standard Operating Procedures (SOP) Manual	A document or set of documents containing detailed instructions for procedures, operations, and activity schedules for IT Operations Management teams(s), department(s) or group(s) to ensure uniformity and consistency.

System Integration Test (SIT)	A technical testing activity to ensure that the Contractor's Solution meets the requirements for integration with other modules.
Takeover	The continuation of a solution and/or services from an incumbent Contract/Contractor.
TennCare	TennCare is the State of Tennessee agency responsible for the administration of the Medicaid and Children's Health Insurance Programs in Tennessee. A list of TennCare programs can be located at: https://www.tn.gov/tenncare/members-applicants/eligibility/categories.html .
TennCare Contractor	Any entity performing services pursuant to a contract with TennCare, including any officer, owner, member, director, employee, volunteer, agent, subcontractor, representative, or assignee of the TennCare Contractor, and any other person, partnership, corporation, or other legal entity performing work or services, or providing materials, under a contract with TennCare for or on behalf of the TennCare Contractor. For purposes of any permitted subcontract, "TennCare Contractor" includes any subcontractor(s), owners, members, officers, directors, partners, employees, and/or agents
TennCare Enterprise Knowledge Management Strategy	As a component of TennCare continuous improvement practices, TennCare has instituted processes that require vendor partners to document project artifacts and best practices. TennCare has established processes for both TennCare and vendor partner's engagement to collaboratively provide knowledge sharing associated with TennCare-designated project engagement activities.
TennCare Integration Standards	TennCare Integration Standards are TennCare-adopted standards developed by the IS Contractor for integrating solutions and components into TennCare's enterprise technical.
TennCare Security and Privacy Offices	The areas of TennCare responsible for oversight of all enterprise solution security and privacy standards.
Tier I – Service Desk	The Tier I – Service Desk is managed by the Integration Services (IS) Contractor and supports general issues, such as receiving initial calls, password reset requests, and identifying incidents. If the request or incident cannot be addressed at the Tier I – Service Desk level, the Tier I – Service Desk is responsible for the routing of higher complexity issues requiring Tier II – Level Support. Additionally, the Tier I – Service Desk is responsible for tracking, recording, and closing every incident.
Tier II – Level Support	Tier II – Level Support requires resources with technical expertise and specialized skills above Tier I – Level Support is usually provided by specialists with deep product knowledge to address incidents such as critical workflow malfunctions or inability to complete a transaction. Once an Incident or Problem has been resolved, or a workaround has been identified, the Tier II – Level Support will report resolution results to the Tier I – Service Desk level.
Tier III – Level Support	Tier III – Level Support requires resources with technical expertise and specialized skills above Tier II – Level Support and is usually provided by specialists with deep product knowledge to address incidents such as critical workflow malfunctions or inability to complete a transaction. Once an Incident or Problem has been resolved, or a workaround has been identified, the Tier III – Level Support will report resolution results to the Tier I – Service Desk level.
Turn-key Solution	A Turn-key Solution is a type of system built end-to-end for TennCare that can be configured and scaled to meet TennCare's business processes.

Turnover	All activities involved in transitioning the Solution responsibilities to TennCare, a designated contractor, and/or successor contractor at the end of the Contract term.
Unit Testing	A testing activity where the Contractor performs technical testing internal to their Solution.
User Acceptance Testing (UAT)	A testing activity carried out by end-users to ensure that the Solution meets business needs from end-to-end.
Verified Community-Based Organization (CBO) Service Location	A CBO Service Location that has confirmed applicable CBO Service Location details (e.g., location address, hours of operation, contact information) are accurate within the Community Resource Directory. A Verified CBO Service Location must have at least one Authorized User associated with that CBO Service Location.
Warranty Defect	Any nonconformance of the goods or services to the terms and conditions of the Contract within the Warranty Period. A Warranty Defect is classified as Critical, High, Medium, and Low and must be resolved in the given timeframe listed in Contract Attachment B, Service Level Agreements and Liquidated Damages.

1.2 Abbreviations

Abbreviation	Definition
24x7x365	Available twenty-four (24) hours per day, seven (7) days per week, and three hundred sixty-five (365) days per year
ACA	Affordable Care Act
ADA	Americans with Disabilities Act
AHC HRSN or AHC	Accountable Health Communities Health Related Social Needs
API	Application Programming Interface
AUP	Acceptable Use Policy
BC/DR	Business Continuity/Disaster Recovery Plan
CAP	Corrective Action Plan
CAQH-CORE	Council for Affordable Quality Healthcare - Committee on Operating Rules for Information Exchange
CBO	Community-Based Organizations
CD	Control Directive
CCT	Care Coordination Tool
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CI	Configuration Item
CIP	Continuous Improvement Process
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CLRS	Closed-Loop Referral System
CM	Control Memorandum
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial Off-the-Shelf

CRISC	Certified in Risk and Information Systems Control
CPO	Central Procurement Office
CPU	Central Processing Unit
CSP	Cloud Service Provider
DDI	Design, Development, and Implementation
DDoS	Distributed Denial of Service
DED	Deliverable Expectation Document
DMZ	Demilitarized Zone
DNS	Domain Name System
DOJ	Department of Justice
DUNS	Data Universal Numbering System
EDI	Electronic Data Interchange
EFFP	Enhanced Federal Financial Participation
EHR	Electronic Health Record
ETL	Extract, Transform, Load
FFATA	Federal Funding Accountability and Transparency Act
FHIR	Fast Healthcare Interoperability Resources
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standard
FTE	Full-Time Equivalent
FTI	Federal Tax Information
FTP	File Transfer Protocols
GIAC	Global Information Assurance Certification
GLBA	Graham-Leach-Bliley Act of 1999
GRC	Governance, Risk, and Compliance
Go-DBE	Governor's Office of Diversity Business Enterprise
GUI	Graphical User Interface
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act
HL7	Health Level Seven
HTML	Hypertext Markup Language
IAM	Identity and Access Management
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Integration Services
ISL	Integration Services Layer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
KPI	Key Performance Indicator
LD	Liquidated Damage
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MCO	Managed Care Organizations

MDM	Master Data Management
MFA	Multi-Factor Authentication
MIC	Medicaid Integrity contractors
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MMP	Medicaid Modernization Program
MMPVP	Medicaid Modernization Program Vendors and Partners
NCPD	Notice of Calculation of Potential Damages
NCPDP	National Council for Prescription Drug Programs
NIAD	Notice of Intent to Assess Damages
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPD	Notice of Potential Damages
O&M	Operations and Maintenance
OCRC	Office of Civil Rights Compliance
OIG	Office of Inspector General
ORR	On Request Report
ORT	Operational Readiness Test
OWASP	Open Web Application Security Project
PC	Personal Computer
PCMH	Patient-Centered Medical Home
PDF	Portable Document Format
PERM	Payment Error Rate Measurement
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Project Management Office
PMP	Project Management Professional
POA&M	Plan of Actions and Milestones
PPACA	Patient Protection and Affordable Care Act
PRAPARE	Protocol for Responding to and Assessing Patients' Assets, Risks, and Experiences
RACI	Responsible, Accountable, Consulted, and Informed
RDA	Records Disposition Authorization
RFP	Request for Proposals
RTM	Requirements Traceability Matrix
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network and Security.
SCA	Security Control Assessment
SDOH	Social Determinates of Health
SFTP	Secure (Shell) File Transfer Protocol
SIEM	Security Incident Event Management
SILC	Solution Implementation Lifecycle
SIT	System Integration Test

SLA	Service Level Agreement
SMP	Subject Matter Professional
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOP	Standard Operating Procedure
SPMO	Strategic Program Management Office
SQL	Structured Query Language
SSA	United States Social Security Administration
SSO	Single Sign-On
SSP	System Security Plan
STS	Strategic Technology Solutions
TARB	Technical Architecture Review Board
TCA	Tennessee Code Annotated
TCRS	Tennessee Consolidated Retirement System
THL	Tennessee Health Link
T-MSIS	Transformed Medicaid Statistical Information System
UAT	User Acceptance Testing
USC	United States Code
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines
WS	Web Service
XLS	Filename Extension (Microsoft Excel spreadsheet file)
XML	Extensible Markup Language



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 37228 and _____

Aunt Bertha, a Public Benefit Corporation dba Findhelp ("Business Associate"), located at 3616 Far West Blvd. Suite 117-454 Austin, Texas 78731

_____, 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 "State Contract" or "State Contracts."

LIST OF STATE CONTRACTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT:

TN State Contract 80732

In the course of performing services under the State Contract(s), Business Associate may come into contact with, use, or disclose Protected Health Information ("PHI"). Said State Contract(s) is/are hereby incorporated by reference and shall be considered part of this Agreement as if the State Contract(s) was/were fully included 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 agree to establish satisfactory assurances that Business Associate will appropriately safeguard PHI that Business Associate receives from or on behalf of Covered Entity, and therefore, the Parties execute this Agreement.

In the case of any conflict, discrepancy, or ambiguity, between this Agreement and the State Contract(s), this Agreement shall govern as relating to the conflict, discrepancy, or ambiguity only. Absent any conflict, discrepancy, or ambiguity between this Agreement and the State Contract(s), the State Contract governs.

1. DEFINITIONS

All capitalized terms used but not otherwise defined in this Agreement shall have the same meaning as the defined terms in 45 C.F.R. Parts 160 through 164, or other applicable law or regulation. A reference in this Agreement to the Privacy or Security Rule means the rule or section as in effect as of the date of this Agreement or as amended after the execution of this Agreement.

1.1 “Commercial Use” means obtaining PHI with the intent to sell, transfer or use it for commercial or personal gain, or malicious harm; selling to a third party for consumption, resale, or processing for resale; applying or converting 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 presentation, conference, or meeting setting, with a goal of obtaining or gaining 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 Business Associate under this Agreement. Any information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, relating to any individual enrolled in the TennCare program (“TennCare Enrollee”), or relating to individual(s) who may potentially enroll in the TennCare program, provided to or obtained through Business Associate’s performance under this Agreement, shall also be treated as Confidential Information to the extent that confidential status is afforded under state and federal laws or regulations to the information provided to, or obtained through, Business Associate’s performance. All Confidential Information shall not be subject to disclosure under the Tennessee Public Records Act.

1.3 “Electronic Signature(s)” 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 shall include the act or process of promoting, selling, leasing, or licensing any TennCare information or data for profit, advantage, benefit, or similar goal, 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 State Contract(s), or as required by law.

2.2 HIPAA and HITECH Compliance. HITECH and its implementing regulations impose requirements on business associates with respect to privacy, security, and Breach notification. Business Associate hereby acknowledges and agrees that it is functioning as a Business Associate of Covered Entity as obligated by this Agreement and the State Contract(s). Business Associate further acknowledges that it shall comply with any applicable provisions of HIPAA and HITECH. Business Associate and 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. Even if a provision of HIPAA or HITECH is not specifically set forth in this Agreement, all applicable provisions of HIPAA and HITECH are incorporated into this Agreement in their entirety.

2.3 Business Management. Business Associate may use and disclose PHI for the proper management and administration of 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 State Contract(s), or as otherwise required by law, and is prohibited from uses or disclosures of PHI that would not be permitted if done by 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 State Contract(s), this Agreement, or as required by law. This includes the implementation of Administrative, Physical, and Technical Safeguards to appropriately protect Covered Entity’s PHI against any reasonably anticipated threats or hazards utilizing the technology commercially available to Business Associate (See also Agreement Section 3.2). Business Associate shall maintain, and provide

to TennCare when requested, appropriate documentation of Business Associate's compliance with the Privacy Rule, except when Business Associate is required by TennCare policies and procedures to provide compliance documents on an established timeframe without request from TennCare. Appropriate documentation of compliance with the Privacy Rule includes, but is not limited to, Business Associate's policies and procedures, records of training, records of breaches, and sanctions of members of its Workforce.

2.5 Privacy Provisions in 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 Business Associate involving the use, custody, disclosure, creation of, or access to, PHI or other confidential TennCare information, to enter into a written contract that is substantially similar to this Agreement with respect to all privacy provisions. Said substantially similar written contract shall not include less stringent terms or restrictions than this Agreement with Business Associate with respect to the privacy provisions, except for Agreement Section 4.4.2, which shall only apply to Business Associate notwithstanding the requirements in this Agreement 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. Business Associate also agrees to consult with TennCare about any mitigation efforts.

2.7 Reporting of Violations and Reasonably Suspected 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, or upon reasonable suspicion, of any use or disclosure or reasonably suspected use or disclosure of PHI in violation of, or otherwise not provided by, this Agreement. Business Associate shall make its report to Covered Entity immediately upon becoming aware of any use or disclosure or reasonably suspected use or disclosure of PHI not provided by this Agreement, and in no case shall the Business Associate take longer than twenty-four (24) hours to report the discovery to Covered Entity. Reports shall be submitted as provided for in Agreement Section 3.5.

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 or a suspected Breach of Unsecured PHI immediately upon becoming aware or upon reasonable suspicion of the Breach, and in no case later than twenty-four (24) hours after becoming aware or upon reasonable suspicion. Notice shall be submitted as provided for in Agreement Section 3.5.

2.8.2 Business Associate shall cooperate with Covered Entity by timely providing the appropriate and necessary information to Covered Entity, as reasonably anticipated or otherwise requested by Covered Entity.

2.8.3 Covered Entity shall make the final determination on 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. In the event an Individual requests access to PHI and Business Associate's participation is necessary to comply with the request, Business Associate agrees to timely respond as further outlined below.

2.9.1 Requests Submitted to Covered Entity that Require Business Associate's Participation. Covered Entity shall forward to Business Associate in a timely manner any Individual's request for access to or a copy of the Individual's PHI, in any form the Individual chooses if the PHI is readily

producible in that format.

2.9.2 Requests Submitted to Business Associate.

- (a) 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 to meet the requirements of 45 C.F.R. § 164.524.
- (b) 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 Business Associate, Business Associate will provide the requested copy to the Individual as specified in 2.9.3(a). If Business Associate provides copies of PHI to the Individual, it may charge a reasonable fee for the copies as permitted by applicable regulations. Business Associate is permitted to send to an Individual or Individual's designee unencrypted emails including Electronic PHI if the Individual requests it, provided Business Associate has advised the Individual of the associated risk and the Individual still chooses to receive the message by unencrypted email.
- (c) If Business Associate receives a request for PHI not in its possession and in the possession of 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 timely.

2.9.3 Timeframes for Response.

- (a) The Parties understand that if either Party receives a request for access to or copies of PHI from an Individual that the Party may complete with only its own onsite information, the time for providing a response to the Individual shall be no more than thirty (30) days, or a timeframe otherwise in compliance with 45 C.F.R. § 164.524. Business Associate shall also notify Covered Entity upon completion of the request.
- (b) If Covered Entity receives a request from an Individual for access to or copies of PHI, and requires information from Business Associate in addition to Covered Entity's onsite information to fulfill the request, Business Associate shall have no more than fifteen (15) days, from the date of Covered Entity's notice, to provide access or deliver such information to Covered Entity so that 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 responsible for responding to the Individual's request for access to or copies of PHI is unable to complete the response to the request in the required timeframe, the responsible 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 one (1) time for no more than thirty (30) additional days.

2.10 Individual's Request to Amend PHI. If Business Associate receives PHI from Covered Entity in a Designated Record Set and an Individual requests to amend PHI, 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. Business Associate shall make the amendment promptly in the time and manner designated by Covered Entity and shall notify Covered Entity upon completion. Business Associate shall have thirty (30) days from Covered Entity's notice to complete the amendment to the Individual's PHI.

2.11 Recording of Designated Disclosures of PHI. Business Associate shall document any and all disclosure(s) 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.

2.12 Accounting for Disclosures of PHI. In the timeframe and manner designated by Covered Entity, Business Associate agrees to provide to Covered Entity, or an Individual or Individual's designee, information

collected in accordance with this Agreement to enable Covered Entity to respond to a request from an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Covered Entity shall forward the Individual's request requiring the participation of Business Associate to Business Associate in a timely manner, after which Business Associate shall provide the accounting of disclosures of PHI to Covered Entity as follows:

- (a) If Covered Entity directs Business Associate to provide an accounting of disclosures of the Individual's PHI directly to the Individual, Business Associate shall have sixty (60) days from the date of the Individual's request to provide access or deliver such information to the Individual or Individual's designee. Covered Entity shall provide notice to Business Associate in time to allow Business Associate a minimum of thirty (30) days to timely complete the Individual's request.
- (b) If Covered Entity elects to provide the accounting to the Individual, Business Associate shall have thirty (30) days from the date of Covered Entity's notice requesting information for the Accounting to Covered Entity so that Covered Entity may timely respond to the Individual within the sixty (60) day period.
- (c) If either Party is unable to complete the response to the request in the timeframes provided in 2.12(a) or 2.12(b), the Party to complete the response 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 to Individual or Individual's designee one (1) time 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 or Individual's designee without charge. The Parties may charge a reasonable, cost-based fee, for each subsequent request for an accounting by or regarding the same Individual if Individual or Individual Designee is provided notice and the opportunity to modify the request. Such charges shall not exceed any applicable State statutes or rules.

2.13 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. Reasonable efforts may include, but are not limited to, application of recognized industry standards on data minimization and retention privacy controls.

- 2.13.1 Business Associate represents to Covered Entity that all Business Associate's uses and disclosures of, or requests for, PHI shall be the minimum necessary in accordance with the Privacy Rule requirements.
- 2.13.2 Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure from Business Associate as the minimum necessary for the stated purpose.
- 2.13.3 Business Associate shall adequately and properly maintain all PHI received from, or created or received on behalf of, Covered Entity. Properly maintaining PHI shall include, but is not limited to, use of reasonable efforts to timely deidentify or destroy PHI Business Associate receives that is irrelevant or unnecessary for the purposes of this Agreement and any State Contract(s).

2.14 Privacy Compliance Review Upon Request. Business Associate agrees to provide its internal practices, books and records, and policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, to Covered Entity or the Secretary of the United States

Department of Health in Human Services or the Secretary's designee, in a timeframe and manner designated by the requester for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

2.15 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 of the Security Rule applicable to "Business Associates", as the term is defined in the Security Rule. In the case of any conflict, ambiguity, or discrepancies in language between this Agreement and the State Contract(s), this Agreement governs as to the applicable conflict, ambiguity, or discrepancies in language. If no conflict, ambiguity, or discrepancy in language exists, the State Contract governs.

3.2 Security Safeguards and Policies. Business Associates shall implement and maintain information security policies that comply with the HIPAA Security Rule. 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 Covered Entity as required by the Security Rule. This includes specifically, but is not limited to, the utilization of technology commercially available to Business Associate to protect Covered Entity's PHI against any reasonably anticipated threats or hazards. 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, entities, programs, or applications, and devices access its computing systems and information storage, and that only authorized transactions are allowed. 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 or subcontractor to whom Business Associate provides Electronic PHI received from, maintained, or created for Covered Entity, or that carries out any duties for Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, shall execute a contract with Business Associate (or the appropriate equivalent if the agent is a government entity) that is substantially similar to this Agreement with no less stringent restrictions and conditions as the security provisions are in this Agreement, except for the provision in Section 4.4.2.

3.4 Reporting of Security Incidents. Business Associate shall track all Security Incidents as defined and as required by HIPAA and shall periodically report a summary of the Security Incidents as may be requested by Covered Entity. For the purposes of reporting, Covered Entity shall not consider as Security Incidents, external activities (e.g., port enumeration) 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. 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, Business Associate shall expediently notify Covered Entity's Privacy Officer of any related Security Incident immediately upon becoming aware or upon reasonable suspicion of any unauthorized acquisition, including but not limited to, the use, disclosure, modification, or destruction of PHI, by an employee or otherwise authorized or unauthorized user of its system.

3.4.1 Business Associate identifies the following key contact person(s) for all matters relating to this Agreement:

Kraig Dalton -- Director, State Accounts

kdalton@findhelp.com

(304) 761-4727

Business Associate shall notify Covered Entity in writing of any change in the key contact(s) during the term of this Agreement within ten (10) business days of the change.

3.5 TennCare Contact for Privacy and Security Incident Notice. Notification for the purposes of Agreement Sections 2.7, 2.8 and 3.4 shall be made in writing immediately upon becoming aware, or upon reasonable suspicion, of the event. Written notice may be submitted via TennCare's privacy incident reporting form if accessible to Business Associate, email, certified mail, or overnight parcel to:

Division of TennCare
Attention: Privacy Office
310 Great Circle Rd.
Nashville, Tennessee 37243
Phone: (866) 797-9469
Email: Privacy.TennCare@tn.gov

3.6 Security Compliance Review upon Request. Business Associate shall provide its internal practices, books, records, and policies and procedures relating to the security of Electronic PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to Covered Entity or 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 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. 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 the State Contract(s), provided that such use or disclosure would not violate the Privacy and Security Rule if done by Covered Entity.

4.2 Business Associate Uses of PHI. Except as otherwise limited in this Agreement, Business Associate may disclose PHI as required for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that the disclosures are required by law and are also permitted by this Agreement and the State Contract(s). Nothing in this Agreement Section 4.2 permits, or should be construed as permitting, the Business Associate to use PHI for Marketing or Commercial Use.

4.3 Third Party Disclosure Confidentiality. If Business Associate discloses any PHI to a third party for a purpose permitted under 4.2, Business Associate agrees that it 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 PHI except as required by law or for the purpose for which it was disclosed; and (b) notify Business Associate of any instances where third party becomes aware that the confidentiality, integrity, and/or availability of

the PHI is Breached.

4.4 Prohibited Uses and Disclosures. Nothing in this Agreement shall authorize Business Associate to share, use or disclose PHI via any form or medium for the purposes outlined in Agreement Subsections 4.4.1 through 4

4.4.1 Marketing and Commercial Use. Business Associate shall not share, use, or disclose PHI for the purposes of selling, Marketing, or any Commercial Use, or for any purpose construed by Covered Entity as the selling, Marketing, or Commercial Use of TennCare Enrollee personal or financial information with affiliates or otherwise, even if such sharing would be permitted by federal or state laws.

4.4.2 Offshore Disclosure. Business Associate shall not share, use, or disclose PHI with any third party beyond the boundaries and jurisdiction of the United States without express written authorization from Covered Entity.

4.4.3 Genetic Information for Underwriting Purposes. Business Associate shall not use or disclose PHI that is Genetic Information for underwriting purposes.

4.4.4 Other Uses and Disclosures Strictly Prohibited. Nothing in this Agreement shall permit Business Associate to share PHI with Business Associate's affiliates, contractors, subcontractors, or other third parties, except for the purposes of the State Contract(s) identified in the "LIST OF STATE CONTRACTS 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 Information by Business Associate, its subcontractors, its affiliates, or Contractors, other than the use permitted for the purposes of this Agreement, shall require express written authorization by Covered Entity, and a Business Associate Agreement or amendment as necessary. Activities which are prohibited include, but are not limited to, Marketing, 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 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 Business Associate complies with the obligations in Agreement Section 3.2 and this Agreement. 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.

4.7 Limitation on Permitted Uses and Disclosures. Business Associate will limit the uses and disclosures 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. Covered functions for purposes of this Agreement Section 4.7 shall include business planning and development, such as: conducting cost-management and planning-related analysis related to managing and operating Business Associate's functions; formulary development and administration; development and improvement of methods of payment or coverage policies; and 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. The listed covered functions shall only be permitted if PHI is not disclosed, and disclosure is not prohibited pursuant to any other provisions in this Agreement.

5. OBLIGATIONS OF COVERED ENTITY

5.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the Covered Entity's notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, as well as any changes to the notice of Privacy Practices. Notice may be provided via publication on TennCare's website.

5.2 Notice of Changes in Individual's Authorization for Access to 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 to 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 Agreement Sections 5.2 through 5.3 are 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 on the date of the last signatory, or on the signature date if all Parties sign on the same day, and shall terminate when all PHI, regardless of form, provided 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 mutually agree in writing that it is unfeasible to return or destroy PHI, Agreement Subsection 6.3.5 below applies.

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 any State Contracts 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. Nothing in Agreement Section 6.2 limits the State's ability to terminate the State Contract as permissible under the State Contract.

6.2.1 Upon Covered Entity's knowledge of a breach by Business Associate of the terms of this Agreement or any State Contract (s), 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. If Business Associate does not cure the breach or end the violation within the reasonable time following notice, as specified by Covered Entity, Covered Entity shall terminate this BAA; 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 Agreement Subsections 6.3.2 and 6.3.5, 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 subcontractors or agents of Business Associate.

6.3.1 Business Associate shall consult with Covered Entity as necessary to ensure an appropriate means of return or destruction of PHI and Confidential Information and shall notify Covered Entity in writing when such destruction is complete. If PHI or Confidential Information is to be returned, the Parties shall document when all information has been received by Covered Entity.

6.3.2 Agreement 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 Business Associate if the method of such archiving reasonably protects the continued privacy and security of such information and Business Associate obtains written approval at the time of archival from Covered Entity.

Otherwise, neither Business Associate nor its subcontractors and agents shall retain copies of TennCare Confidential Information including enrollee PHI, except as provided herein in Agreement Subsection 6.3.5.

6.3.3 The Parties agree to anticipate the return or the destruction of PHI and other 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. Business Associate shall notify Covered Entity whether it intends to return or destroy the PHI or Confidential Information with additional detail as requested by Covered Entity. In the event Business Associate determines that returning or destroying the PHI and other Confidential Information received by or created for Covered Entity at the end or other termination of the State Contract(s) 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, for the renewal or amendment of those same agreements, or for other unavoidable circumstances, the Parties contemplate that PHI and other Confidential Information of 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 Covered Entity at the conclusion of any State Contract(s), or otherwise make an express alternate agreement consistent with the provisions of Agreement Section 6.3 and its Subsections.

6.3.5 Upon written mutual agreement of the Parties that the return or destruction of PHI or Confidential Information 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 Amendment. The Parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate 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.

7.2 Survival. The respective rights and obligations of Business Associate under applicable confidentiality provisions and Agreement Sections 4 and its Subsections, and 6.3 and its Subsections, shall survive the termination or expiration of this Agreement.

7.3 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the Privacy and Security Rules.

7.4 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.

7.5 Notices and Communications. Except as specified in Agreement Section 3.5, 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 Agreement Section 7.6, 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 relating to Agreement Sections 2.7, 2.8 and 3.4 of this Agreement need only be reported to the Privacy Office pursuant to Agreement Section 3.5.

COVERED ENTITY:

Stephen Smith, Director
Division of TennCare
310 Great Circle Rd.
Nashville, TN 37243
Fax: (615) 253-5607

BUSINESS ASSOCIATE:

Aunt Bertha, a Public Benefit Corporation
Attn: Findhelp Compliance and Legal Teams
3616 Far West Blvd. Suite 117-454
compliance@findhelp.com
legalnotices@findhelp.com

All instructions, notices, consents, demands, or other communications shall be considered effectively given as follows: on the date of hand delivery; on the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing by first class mail postage prepaid; 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; or via electronic submission as approved or as directed by TennCare.

7.6 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 Business Associate to transmit such deliverables in the manner specified by Covered Entity may, at the option of Covered Entity, result in liquidated damages as set forth in one (1) or more of the State Contracts 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.

7.7 Strict Compliance. No failure by any Party to insist on 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 on strict compliance, exercise that option, enforce that right, or seek that remedy with respect to the 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.

7.8 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. If any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement and all other provisions of this Agreement shall remain in full force and effect.

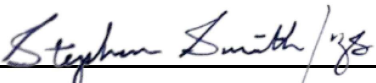
7.9 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that Tennessee law has been pre-empted by HIPAA and HITECH and without giving effect to principles of conflicts of law.

7.10 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 State Contract(s) referenced herein.

7.11 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 Electronic Signatures is valid as an executed Agreement.

IN WITNESS WHEREOF, the Parties execute this Agreement to be valid and enforceable from the latest dated signature set out below or on the date of signatures if both Parties sign on the same date:

DIVISION OF TENNCARE

By: 

Stephen Smith, Director

Date: 5/26/2026

Division of TennCare
310 Great Circle
Road Nashville, TN
37243

Fax: (615) 253-5607

BUSINESS ASSOCIATE

By: 
254356C8F99592C77D22E840DBA367C8 contractworks

Erine Gray - President & CEO

Date: ~~05/26/2026~~

Aunt Bertha, a Public Benefit Corporation d.b.a. Findhelp
3616 Far West Blvd, Suite 117-454
Austin, TX 78731



CONTRACT

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

Begin Date December 1, 2023	End Date November 30, 2026	Agency Tracking # 31865-00635	Edison Record ID 80732			
Contractor Legal Entity Name Aunt Bertha, A Public Benefit Corporation d.b.a findhelp			Edison Vendor ID #0000250024			
Goods or Services Caption (one line only) MMIS – CLRS						
Contractor ☒ Contractor		CFDA # 93.778				
Funding —	FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
	2024	\$21,825.00	\$196,425.00			\$218,250.00
	2025	\$232,800.00	\$1,003,950.00			\$1,236,750.00
	2026	\$467,055.00	\$1,584,495.00			\$2,051,550.00
	2027	\$261,900.00	\$829,350.00			\$1,091,250.00
	TOTAL:	\$983,580.00	\$3,614,220.00			\$4,597,800.00
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: For Profit						
Selection Method & Process Summary (mark the correct response to confirm the associated summary) ☒ Competitive Selection Competitive Procurement RFP 31865-00635 ☐ Other						
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 G. Allen Digitally signed by: Crystal G. Allen DN: CN = Crystal G. Allen email = Crystal.G.Allen@tn.gov C = US O = TennCare OU = Budget Date: 2023.10.18 10:23:55 -06'00'						
Speed Chart (optional) TN00000736 – DDI TN00000738 – O&M		Account Code (optional)				

**CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF FINANCE AND ADMINISTRATION,
DIVISION OF TENNCARE
AND
AUNT BERTHA, A PUBLIC BENEFIT CORPORATION
D.B.A. FINDHELP**

This Contract, by and between the State of Tennessee, Department of Finance and Administration, Division of TennCare ("State" or "TennCare") and Aunt Bertha, a Public Benefit Corporation d.b.a. findhelp® and findhelp.org ("Contractor"), is for the provision of the Closed-Loop Referral System (CLRS), 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 Public Benefit Corporation
Contractor Place of Incorporation or Organization: Delaware
Contractor Edison Registration ID #0000250024

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 abbreviation shall be as set forth in Attachment A, Definitions and Abbreviations.
- A.3. The Contractor shall provide TennCare with a cloud-native Closed-Loop Referral System Software as a Service (SaaS) Solution. The Solution shall incorporate current Industry Standard tools and technology; shall be adaptable and scalable to accommodate current trends, technological advances, and regulatory requirements; and shall be hosted in commercial public cloud infrastructure.
 - A.3.1. The Contractor shall provide a Solution inclusive of all hardware, software, cloud, and infrastructure costs required to acquire, install, operate, and maintain the Solution.
- A.4. 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, through the Control Memorandum (CM) process, 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 and designated representative enterprise vendors, minimally including Managed Care Organizations (MCOs), Providers, Community-Based Organizations (CBOs), Care Coordination Tool (CCT) Contractor, and Medicaid Modernization Program Vendors and Partners (MMPVP) as necessary or at the request of TennCare, to coordinate and complete required activities and Deliverables. The Contractor shall coordinate with TennCare to complete training services specific to the Contractor's Solution through all phases of the Contract.
 - A.4.3. 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) Phase: The Contractor shall design, develop, and implement a Solution. The implemented Solution shall:

- A.5.1.1. Meet the service and delivery timelines for the Solution in accordance with Phase 1 - Phase 2 as specified in RFP #31865-00635 Figure 1 – Closed-Loop Referral System Timeline as specified and approved by TennCare in Contractor's project schedule. Any variances from these timelines, for any reason and whether approved by TennCare or not, shall not result in additional cost(s) to TennCare.
- A.5.1.2. Meet all Functional Requirements described in Section A.6.
- A.5.1.3. Meet all Non-Functional Requirements described in Section A.7. through A.14.
- A.5.1.4. Comply with all Service Level Agreements (SLAs) defined in Attachment B - Service Level Agreements and Liquidated Damages.

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

- A.5.2.1. At the conclusion of DDI Phase 1 and DDI Phase 2, the Contractor shall operate and maintain the Solution as required by the O&M Phase, outlined in Section A.11.5.
- A.5.2.2. The Contractor shall operate a Module Support Team for the Solution as required by Section A.11.10.2.

A.6. Closed-Loop Referral System. The Contractor shall provide and operate a cloud-based Solution that meets all requirements in this Section A.6.

A.6.1. Non-Medical Needs Assessment

- A.6.1.1. The Solution shall, at a minimum, offer the following multiple Non-Medical Needs Assessments: Protocol for Responding to and Assessing Patients' Assets, Risks, and Experiences (PRAPARE), Accountable Health Communities Health Related Social Needs (AHC-HRSN or AHC), Health Leads Social Needs Screening Toolkit, and others identified or developed as requested by TennCare during system design.
- A.6.1.2. The Solution shall validate Member enrollment for every Member prior to establishing and completing the Non-Medical Needs Assessment.
- A.6.1.3. The Solution shall close an active Non-Medical Needs Assessment upon disenrollment of TennCare coverage.
- A.6.1.4. The Solution shall have only one (1) active Non-Medical Needs Assessment per Member.
- A.6.1.5. The Solution shall populate a notification if a Member has an active Non-Medical Needs Assessment that prevents the Authorized User(s) from completing multiple active Non-Medical Needs Assessments.
- A.6.1.6. The Solution shall allow Authorized User(s) to submit a complete or incomplete Non-Medical Needs Assessment with Member-supplied information or responses.

- A.6.1.7. The Solution shall alert Authorized User(s) of incomplete data entry fields or inappropriately completed data entry fields when submitting a Non-Medical Needs Assessment.
- A.6.1.8. The Solution shall manage Authorized User(s) access for attributed Members' Non-Medical Needs Assessments.
- A.6.1.9. The Solution shall allow Authorized User(s) to answer the Non-Medical Needs Assessments on behalf of the Member.
- A.6.1.10. The Solution shall allow Authorized User(s) to access the Non-Medical Needs Assessment via a web domain.
- A.6.1.11. The Solution shall allow Authorized User(s) to access the Non-Medical Needs Assessment via a mobile-responsive web domain.
- A.6.1.12. The Solution shall have the capability to integrate Industry Standard ICD-10 Z-codes, including current and future iterations, and associate the external selected diagnosis code with an active Non-Medical Needs Assessment.
- A.6.1.13. The Solution shall auto-populate Non-Medical Needs Assessment data from an integrated Electronic Health Record (EHR) or MCO case management system, when available.
- A.6.1.14. The Solution shall allow for Authorized User(s) to import and populate a Non-Medical Needs Assessment that was completed external to the Solution, in a TennCare specified format.

A.6.2. Community Resource Directory

- A.6.2.1. The Solution shall house a Community Resource Directory, which is a list of CBOs that may be able to assist a Member with the Member's Non-Medical Risk Factor(s).

A.6.2.2. Community Resource Search Capabilities

- A.6.2.2.1. The Solution shall provide multiple criteria for Authorized User(s) to search for a CBO including, but not limited to, Domain, available resources, and geographic location.
- A.6.2.2.2. The Solution shall automatically match CBOs based on the completed Non-Medical Needs Assessment and Domains (e.g., housing, transportation).

A.6.2.3. Community Resource Identification

- A.6.2.3.1. The Solution shall allow Authorized User(s) to select one (1) or more CBO(s) to initiate a Member Referral.
- A.6.2.3.2. The Solution shall have the capability to send electronic notifications to Authorized User(s) on the Referral to include status, updates, or other TennCare-specified criterion.
- A.6.2.3.3. The Solution shall identify and populate CBOs available to the Member based on Domains (e.g., housing, transportation).

A.6.2.3.4. Non-Authenticated Access

- A.6.2.3.4.1. The Solution shall allow Non-Authenticated User(s) to access the public-facing Community Resource Directory.

A.6.2.4. Community Resource Directory Maintenance and Support

- A.6.2.4.1. The Contractor shall provide a Community Resource Directory that complies with the requirements of this Section A.6.2., prior to DDI Phase 1 Go-Live, as specified and approved by TennCare's Contractor project schedule.
- A.6.2.4.2. The Contractor shall provide and maintain a Community Resource Directory within the Solution to contain CBO information by CBO Service Location including, but not limited to, hours of operation, address, service eligibility requirements, capacities, and limitations.
- A.6.2.4.3. The Solution shall have the ability for Authorized User(s) and Non-Authenticated User(s) to flag missing or incorrect information in the Community Resource Directory.
- A.6.2.4.4. The Contractor shall address all flagged items within the Community Resource Directory in accordance with Attachment B, Service Level Agreements and Liquidated Damages.
- A.6.2.4.5. The Contractor shall work with CBOs and TennCare to update the Community Resource Directory information no less than every three (3) months in accordance with Attachment B, Service Level Agreements and Liquidated Damages.
- A.6.2.4.6. The Solution shall have the capability for an Authorized User associated with a CBO Service Location to confirm the accuracy of all applicable organization and program details including, but not limited to: services offered, service area, eligibility criteria, and operating hours.
- A.6.2.4.7. The Solution shall require CBO Service Locations to be confirmed for accuracy, at a minimum, on a three-month interval.
- A.6.2.4.8. The Solution shall only count a CBO Service Location once if a CBO does not have a physical location in the State of Tennessee which provides services to a TennCare Member.
- A.6.2.4.9. The Solution shall have the capability to track statuses and changed statuses per CBO Service Location (e.g., Verified CBO Service Location, Active CBO Service Location).
- A.6.2.4.10. The Solution shall have the capability to record when and how a CBO has been contacted by the Contractor for confirming accuracy of CBO Service Locations.

A.6.3. Non-Medical Risk Factors Referral System

A.6.3.1. Member Enrollment

- A.6.3.1.1. The Solution shall validate Member enrollment for every Referral made prior to creating the Referral.
- A.6.3.1.2. The Solution shall close all open Referrals for a Member upon disenrollment of TennCare coverage.
- A.6.3.1.3. The Solution shall update the Referral close reason upon disenrollment of a Member's TennCare coverage.

A.6.3.2. Closed-Loop Referrals

- A.6.3.2.1. The Solution shall allow an Authorized User to generate a Member Referral to receiving CBO(s).

A.6.3.2.2. The Solution shall notify the Authorized User(s) throughout the entire Referral process with updates regarding the Referral whenever an action is taken, or at a cadence determined by TennCare.

A.6.3.2.3. The Solution shall allow Authorized User(s) to close a Referral irrespective of whether the Member is serviced or if the Member's Non-Medical Needs are met.

A.6.3.2.4. Outgoing Referral Capabilities

A.6.3.2.4.1. The Solution shall allow for the Authorized User(s) to complete a Referral.

A.6.3.2.4.2. The Solution shall notify the Authorized User(s) that the Referral was successfully sent to the CBO for services.

A.6.3.2.4.3. The Solution shall have the ability to send Referral notes to the Authorized User(s) at a cadence determined by TennCare.

A.6.3.2.4.4. The Solution shall notify the Authorized User(s) regarding the Referral when the Referral has been inactive (e.g., a Referral is not accepted, a Referral is not serviced) for a time period defined by TennCare.

A.6.3.2.5. Incoming Referral Capabilities

A.6.3.2.5.1. The Solution shall allow for the CBO(s) to receive electronic notifications.

A.6.3.2.5.2. The Solution shall allow for the CBO(s) to choose its preferred method of electronic notifications (e.g., email or text) for receiving a new Referral and reminders for outstanding Referrals not accepted/declined (e.g., within the Solution, via email).

A.6.3.2.6. Referral Acceptance

A.6.3.2.6.1. The Solution shall allow CBO(s) to either accept or decline the Referral.

A.6.3.2.6.2. The Solution shall allow for the CBO to provide a reason when declining to provide the referred services for the Member.

A.6.3.2.6.3. The Solution shall notify the Authorized User(s) to select a new resource when the CBO declines the Referral for services.

A.6.3.2.7. Referral Tracking

A.6.3.2.7.1. The Solution shall have the capability for Authorized User(s) to enter and store Non-Medical Needs Assessments, Referral information, and Member demographic information.

A.6.3.2.7.2. The Solution shall allow Authorized User(s) to perform a search by Member identifiers such as full name, partial name spelling, date of birth, social security number, and navigate directly to the selected Member profile from the list of Members when there is more than one match.

A.6.3.2.7.3. The Solution shall have the capability to maintain Referral history for all Referrals and for all Members.

A.6.3.2.7.4. The Solution shall allow Authorized User(s) to add Personally Identifiable Information (PII) required to complete the Referral

detail including, but not limited to, Member nickname, contact information, and Non-Medical Risk Factors.

- A.6.3.2.7.5. The Solution shall store and summarize all active and closed Referrals for each Member by criteria identified by TennCare (e.g., by Referral, by Assessment, by date range).
- A.6.3.2.7.6. The Solution shall have the capability to send demographic information updates to TennCare and the Member-associated MCO system(s) as defined by TennCare, with a preference for real-time data exchange.
- A.6.3.2.7.7. The Contractor shall coordinate with the Master Data Management (MDM) contractor to integrate and configure bi-directional data feeds between the MDM and the Solution.
- A.6.3.2.7.8. The Solution shall allow role-based access to Authorized Users to view, track, and edit Referrals they are associated with.
- A.6.3.2.7.9. The Solution shall allow for the Authorized User(s) to enter notes within the Solution (e.g., notes to the Referral through free-form text boxes).
- A.6.3.2.7.10. The Solution shall notify the Authorized User(s) that the CBO has accepted or declined the Referral for services.
- A.6.3.2.7.11. The Solution shall notify the Authorized User(s) of the reason why the CBO has declined the Referral for services, if provided by the CBO.
- A.6.3.2.7.12. The Solution shall notify the Authorized User(s) of the outcome of the Referral.
- A.6.3.2.7.13. The Solution shall allow for any Authorized User(s) within the Member's care team (including the MCO case manager, Provider, and CBO) to update the Non-Medical Needs Assessments within the Solution and document the results of the Referral.

A.6.4. System Integration

- A.6.4.1. The Solution shall provide self-service mechanisms for external Authorized User(s) to register and login (e.g., login assistance for username and password, forgot password, and password reset).
- A.6.4.2. The Solution shall integrate with TennCare's enterprise Identity and Access Management (IAM) solution to authenticate TennCare staff.
- A.6.4.3. The Contractor shall follow Information Technology Service Management (ITSM) procedures to provide TennCare employees role-based access in order to establish the appropriate use of the Solution.

A.6.4.4. Identity Management

- A.6.4.4.1. The Solution shall authenticate Authorized User(s) external to TennCare based on role assignments and privileges.
 - A.6.4.4.1.1. The Contractor shall provide a TennCare-approved Acceptable Use Policy (AUP) via a web form for all individuals to complete prior to the Contractor granting an individual access to the Solution as an Authorized User.

- A.6.4.4.1.2. The Contractor shall require all individuals to re-sign the AUP on an annual basis to maintain access to the Solution as an Authorized User.
- A.6.4.4.1.3. The Solution shall support parameters and auto-generated reminders for Authorized Users to re-sign the AUP on a TennCare-determined timeframe prior to AUP expiration.
- A.6.4.4.1.4. The Solution shall not allow an individual access to the Solution until the individual signs or re-signs the AUP.
- A.6.4.4.1.5. The Contractor shall generate On-demand reports available to TennCare regarding AUP acknowledgement statistics.

A.6.4.5. Integration Services Layer (ISL) Integration

- A.6.4.5.1. The Solution shall have the capability to receive Member data via the Integration Services Layer (ISL) at a cadence determined by TennCare, no less than daily.
- A.6.4.5.2. The Solution shall have the capability to send all Solution data to the TennCare Data Ecosystem (DE) via the ISL.
- A.6.4.5.3. The Solution shall have the capability to support integration with TennCare-specified Provider's EHRs.
- A.6.4.5.4. The Solution shall have the capability to send Referral updates in a format agreed upon by the Contractor and TennCare, to the MCO case management system and TennCare Provider EHR solutions at a cadence determined by TennCare, no less than daily.
- A.6.4.5.5. The Solution shall have the capability of sending Referral notes directly to the Member-attributed MCO case management system.
- A.6.4.5.6. The Solution shall allow for Authorized Users to attach or upload documents and images, such as, but not limited to, JPEG or PDF, generated from outside sources.
- A.6.4.5.7. The Solution shall allow attached or uploaded electronic files/documents (e.g., MS Word) to be opened by the specified program.

A.6.5. Data Analytics and Reporting

- A.6.5.1. The Solution shall provide the Authorized User(s) with configurable reports based on aging Referrals at a cadence determined by TennCare.
- A.6.5.2. The Solution shall have the ability to configure custom alerts and reports based on Authorized User(s) preferences.
- A.6.5.3. The Solution shall have the ability to run pre-configured, On-demand reports, such as quantitative data analytics and historical reporting.
- A.6.5.4. The Solution shall provide Authorized User(s) a summary of Referral data based on their MCO's Member population.
- A.6.5.5. The Solution shall allow Authorized Users to have the capability to generate pre-configured reports on associated referrals, statuses, and outcomes for associated TennCare Members.

- A.6.5.6. The Solution shall provide analytics on CBOs based on their statuses (e.g., Verified CBO Service Location, Active CBO Service Location) and the number of CBOs enrolled including, but not limited to, services provided, Members seen, number of Referrals accepted and/or rejected, and Grand Regions throughout the State (e.g., East, Middle, West).
- A.6.5.7. The Solution shall produce analytics based on a log of updates to CBO details, including the ability to view reports in a format determined by TennCare.
- A.6.5.8. The Solution shall log and report the number of Authorized User(s) of the Solution, including, but not limited to, type (i.e. Provider or CBO), county, and zip code.
- A.6.5.9. The Solution shall report the number of Referrals made for all Authorized User(s) including metrics such as, but not limited to, type, county, and zip code.
- A.6.5.10. The Solution shall report Member demographic characteristics, including, but not limited to race, ethnicity, preferred language, and Federally-protected classes.
- A.6.5.11. The Solution shall have the capability to generate overall Referral closure reports (e.g., Referrals closed over specific period with reason closed) at a cadence determined by TennCare.
- A.6.5.12. The Solution shall have the capability to generate reports that are suitable to support related grant funding.
- A.6.5.13. The Solution shall have the ability to maintain data and provide data to the DE for storage, reference, and performing advanced analytics.
- A.6.5.14. The Contractor shall collaborate with TennCare's DE Contractor(s) to execute advanced reporting and analytics (e.g., aggregation of data, data modeling, forecasting) using all Solution data to generate ad hoc reports as defined by TennCare. Such analytics and reporting capabilities should leverage the technology and the features available as part of TennCare's DE.
- A.6.5.15. The Solution shall have the ability for Authorized User(s) (e.g., administrators, supervisors) to post system-wide messages.

A.7. Data Governance

- A.7.1. The Contractor shall support TennCare's policies 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 Solution data and information in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards and align with the TennCare Enterprise Data Model.
- A.7.2. The Solution shall prevent unauthorized access, use, abuse, disclosure, disruption, or modification of data without proper TennCare consent.
- A.7.3. The Solution 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 Solution 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 Solution shall capture all data that is used, created, or archived by the Contractor under this Contract for the ownership, right, title, and interest of TennCare. The Contractor shall use and maintain data in the Contractor's cloud environment to support the Services of this Contract.
- A.7.6. 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.7.7. The Contractor shall ensure that the Solution has the ability, at a minimum, to store, archive, retrieve, and purge data according to the applicable TennCare Records Retention Policy and Records Disposition Authorization (RDA) List located in Attachment C, Procurement Library, and as defined by TennCare Data Policies and Standards or agreed upon by TennCare.
- A.7.8. The Solution shall retain all related application, network, system, and perimeter data including logs, files, and records for the required retention period according to the applicable TennCare Records Retention Policy and Records Disposition Authorization (RDA) List located in Attachment C, Procurement Library, and as defined by the TennCare Log Data Retention Policy based on the type of log files and the type of data contained within the log files or as defined by TennCare.
- A.7.9. The Contractor shall maintain logs that are readily accessible to TennCare staff at no cost for the required retention period as defined by the TennCare Log Data Retention Policy based on the type of log files and the type of data contained within the log files 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.
- A.7.10. 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.7.11. 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.7.12. The Solution 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.7.13. 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.7.14. The Contractor shall support governance capabilities such as Metadata management, Data Quality, and Master Data Management (MDM) in accordance with the TennCare Data Governance standards as defined by 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 Solution shall be hosted in a public cloud-hosted environment.
 - A.8.1.1.2. The Solution shall include all environments necessary to develop and test changes to the Solution and to support the testing of the Solution in accordance with the TennCare Solution Implementation

Lifecycle (SILC) Standard located in Attachment C, Procurement Library.

- A.8.1.1.3. The Contractor shall minimize dependence on traditional IT infrastructure, with the ability to procure off-premise (non-State hosted) solutions and services that leverage delivery mechanisms such as SaaS.
- A.8.1.1.4. The Contractor shall work with TennCare and State of Tennessee Strategic Technology Solutions (STS) to determine the secure Domain Name System (DNS) solution including strategy, design, implementation, infrastructure, and ongoing maintenance that allows proper forwarding between the Solution and the State datacenter.
- A.8.1.1.5. The Contractor shall determine the network and bandwidth requirements for the Solution and work with the IS Contractor, as applicable, for the design and setup of network connectivity required between the Solution and State datacenter in collaboration with and approved by TennCare.
- A.8.1.1.6. The Contractor shall communicate in writing to TennCare the overall approach to cloud hosting, including systems and operations under the auspices of subcontractors, at the request of TennCare.
- A.8.1.1.7. The Contractor shall deliver the Solution as a Turn-key Solution and configure On-demand to scale for use by TennCare.
- A.8.1.1.8. 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.10.b)1); exceptions to the agreed-upon schedule shall be approved by the State.
- A.8.1.1.9. The Solution shall support both DNS name-based whitelisting as well as IP based.
- A.8.1.1.10. The Contractor shall support any cut-over activities of the existing functionality related to the Solution, including, but not limited to, a one-time load (conversion) of data per the TennCare Data Conversion Standard and TennCare Project Management Plan Standard, located in Attachment C, Procurement Library.

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. 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 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, MMPVP, MCOs, Providers, 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 Attachment B, Service Level Agreements and Liquidated Damages. 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 Attachment B, Service Level Agreements and Liquidated Damages, 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.
- 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.
- A.8.3.2. The Contractor shall perform incremental and full backups of the Solution 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.

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

A.9. Technical Requirements

A.9.1. Technology Standards

- A.9.1.1. The Contractor shall ensure that the Solution is able to handle current and future standards and requirements including, but not limited to: ICD-10 Z codes including any future versions, 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 Solution shall provide a flexible framework that allows the import and export of data using industry-standard secured and encrypted File Transfer Protocols (FTP).
- A.9.1.3. The Solution 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 located included in Attachment C, Procurement Library.
- A.9.1.5. The Solution shall align with the CMS Medicaid Information Technology Architecture (MITA) framework.
- A.9.1.6. The Solution shall comply with all HIPAA standard Transactions and Code Sets (TCS) as mandated by TennCare and CMS.
- A.9.1.7. The Contractor shall, upon obtaining written authorization from TennCare, implement and support integration with existing TennCare enterprise tools for functions including, but 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.9.1.8. 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, and/or format for TennCare's approval.
- A.9.1.9. The Contractor shall plan and implement tools required for data transfer and ensure that data can be transferred from the Solution to the Integration Services Layer (ISL) at no additional cost to TennCare.
- A.9.1.10. 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.9.1.11. The Contractor shall plan and implement tools required for data archive and ensure that data can be archived and accessible at TennCare's request.

- A.9.1.12. 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.9.1.13. The Contractor shall plan, estimate, and price for 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 Maximum Liability and shall not result in additional cost to TennCare or the State of Tennessee during the Contract Term. Current CLRS Volumetric Information is provided in Attachment C, Procurement Library, for reference purposes.
- A.9.1.14. The Solution shall comply with Industry Standards including, but not limited to, EDI/X12, NIEM, CAQH-CORE, HL7/FHIR, NCPDP, and HIPAA for data interchange.

A.9.2. Accessibility

- A.9.2.1. The Contractor and Solution 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 with a goal to transition to WCAG 3 level silver for the Solution (For the W3C's guidelines see: <https://www.w3.org/WAI/> and <https://www.access-board.gov/ict/>).
- A.9.2.2. The Contractor's accessibility responsibilities shall include ensuring optimization of the Solution 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 Solution's DDI, 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 Solution; understanding the difference between accessible content and conforming content; being aware of the Solution's testing tools and any limitations the tools have for testing accessibility and providing workarounds; and assessing the impact of technology platforms on the Solution (i.e. applications, portals, and be accessible across different platforms).
- A.9.2.3. The Contractor agrees to perform regularly scheduled (i.e., automatic) scans that will occur at a minimum on a monthly basis and manual testing for the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver) 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 accessibility guidelines (WCAG 3.0 Silver). Commercial Off-The-Shelf ("COTS") products may be used to verify the technology solution's compliance with the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver). The reports shall be provided to TennCare's Office of Civil Rights Compliance ("OCRC") for review and approval.
- A.9.2.4. The 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.9.2.5. 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 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.9.2.6. Prior to the start of this Contract and on an annual basis thereafter, the Contractor's staff that is designated to work on the Solution 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, the 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.9.2.7. In the event that the Solution or a component of the Solution fails to comply with the accessibility standards, the Contractor shall develop and submit a noncompliance report to TennCare's OCRC for approval, that identifies the areas of noncompliance, a plan to bring the system or component into compliance, an alternative/work around that provides Authorized Users with the equivalent access to the content, and a timeframe for achieving that compliance. TennCare's OCRC 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's OCRC, 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 the Contractor is unable to obtain content that conforms to the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver), it shall demonstrate through its reporting to TennCare's OCRC that obtaining or providing accessible content would fundamentally alter the nature of its goods and services or would result in an undue burden.
- A.9.2.8. The Contractor agrees to comply with Title VI of the Civil Rights Act of 1964. As part of achieving Title VI compliance, the Contractor shall add a system function that allows Authorized 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.9.2.9. 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 Solution to provide automated system monitoring.

- A.9.3.2. The Solution 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 Solution shall capture all statistics required to measure the contractual SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages, 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 Solution 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 Solution shall provide systematic notifications to identified Authorized User(s).
- A.9.3.7. The Solution shall include ongoing performance monitoring and remediation.
- A.9.3.8. The Solution shall allow Authorized User(s) to view the status of scheduled, submitted, and canceled reports.
- A.9.3.9. The Contractor shall provide tools and a monitoring function to monitor Key Performance Indicators (KPIs) metrics including, 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 Solution 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 Solution shall support monitoring, configuration of alerts, and configuration of notifications based on thresholds defined by TennCare.
- A.9.3.13. The Contractor shall monitor, track, and report to TennCare infrastructure space and storage trends over the term of the Contract, including space and storage for staging the Solution.
- A.9.3.14. The Contractor shall deliver all reporting and analytical requests on a TennCare-approved schedule.
- A.9.3.15. The Solution shall automate routine reports as required by TennCare on a daily, weekly, monthly, annual cadence, or other frequency as required by TennCare. These routine reports will be generated and transported without manual intervention and include notifications to Authorized Users upon completion.

- A.9.3.16. The Solution 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 Solution shall be scalable and adaptable to meet future growth and expansion/contraction needs, such that the Solution can be expanded On-demand and be able to retain its performance levels when adding additional Authorized Users, functions, and storage.
- A.9.4.2. The Solution shall be scalable both horizontally and vertically to support the defined performance SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages.
- A.9.4.3. The Contractor shall produce a Capacity and Performance Plan, included in the Infrastructure Plan, approved by TennCare prior to any infrastructure build and as required by the TennCare Solution Implementation Lifecycle Standard.
- A.9.4.4. The Solution shall be accessible to rural and/or remote communities with limited bandwidth.

A.9.5. Availability

- A.9.5.1. The Solution 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 the application SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages, excluding scheduled downtime, natural disasters, and force majeure, or as agreed to in the Contract.
- A.9.5.3. The Solution 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).
- A.9.5.4. The Contractor shall ensure that the Solution is available 95% of the time, 7:00 am to 9:00 pm CST, and a minimum of five (5) days a week, excluding State observed holidays and TennCare approved planned downtime. The Solution is considered unavailable when any of the capabilities do not function as described in this Contract and ancillary documentation.

A.9.6. Graphic User Interface (GUI)

- A.9.6.1. The Solution 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, Arabic, and Spanish.
- A.9.6.2. If the Solution is supported by the User-access website, the Solution shall be accessible and shall be compatible with all Mainstream Browsers.
- A.9.6.3. The Solution 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 Solution shall facilitate internet/intranet accessible, browser-based web capabilities with no client component download(s) for all Authorized Users.
- A.9.6.5. The Solution 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.9.7. Supportability

- A.9.7.1. The Contractor shall innovate, mature, and improve technology and process capabilities of the Solution 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 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 (CIP) throughout the term of the Contract.
- A.9.7.3. The Contractor shall ensure and demonstrate that the Solution runs on software/hardware Contractor 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 Solution 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 Solution 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, Extract, Transform, and Load (ETL), cloud integration, Data Models and storage, workflows, reporting and analytical engine, and container technologies.
- A.9.7.5. The Solution shall be upgradable while preserving 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 Solution are supported by COTS vendors for the duration of the Contract, including the option years. If the COTS or commercially supported components in the Solution become unsupported by the COTS vendors during the lifetime of the Contract, the COTS or commercially unsupported components in the Solution shall be replaced by the Contractor at no additional expense to TennCare.
- A.9.7.7. The Contractor shall enforce the Enterprise-Wide Data Quality and governance policies and processes defined and approved by TennCare.
- A.9.7.8. The Solution shall provide context-specific help through the User interface. The context-specific help shall refer to specific business rules and shall update automatically when business rules or policies are updated.

A.9.8. Audit/Audit Support

- A.9.8.1. The Contractor shall establish procedures and best practices, in accordance with the audit 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 Solution shall provide 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 Solution 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.
 - 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 Solution shall maintain an audit trail of all actions related to data/content in accordance with the TennCare Enterprise Security Policy and CMS Volume II: ACA Administering Entity System Security and Privacy Plan, located in the Attachment C, Procurement Library, controls which include, but are not limited to:
 - A.9.8.5.1. Date and time data/content entered in the Solution;
 - 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 and/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.9.9. MyTN.gov Interface
- A.9.9.1. TennCare may require the software developed or provided by the Contractor under this Contract to interface with the State's customer-facing portal, MyTN.gov. This may occur at any time during the Term of the Contract. If so, the Contractor may have to comply with one, or more, of the following requirements:
 - A.9.9.1.1. All web applications must be Responsive. "Responsive" is an Industry Standard term that refers to a web design that makes web pages render well on a variety of devices and window or screen sizes. .
 - A.9.9.1.2. All web applications must have the capability to use a Single-Sign On (SSO) server utilizing the following Industry Standard protocols: Security Assertion Markup Language ("SAML") or minimum of OAuth 2.0.
 - A.9.9.2. Any of the obligations in Section A.9.9. that were known and required prior to Contract Effective Date will be specified herein, including necessary compensation methods and amounts.
 - A.9.9.3. For any of the obligations in Section A.9.9. that were unknown or not required at Contract Effective Date, it will be necessary to add lines, items, or options to the Contract to accommodate one or more of the new interface requirements. TennCare shall add these lines, items, or options in accordance with the MOU process described in Section E.4, below. If the Contractor requires additional

compensation for the interface tasks, such compensation shall be negotiated and specified through this same MOU process.

A.10. Security and Privacy

- A.10.1. The Contractor shall review and sign the current version of the Acceptable Use Policy (AUP) prior to accessing the TennCare network and/or data and annually thereafter.
- A.10.2. The Contractor and all sub-contractors shall complete the TennCare information security and privacy training program and submit compliance reports to the TennCare Privacy Officer prior to their accessing TennCare information systems. The Solution shall provide security that is consistent with the requirements of this Contract and with the standards established by the Contractor for the Solution.
- A.10.3. The Contractor and all sub-contractors shall complete the TennCare information security and privacy training program regarding the accessing, disclosing, and securing Federal Tax Information (FTI) and submit compliance reports to the TennCare Privacy Officer prior to their accessing TennCare information systems containing FTI.
- A.10.4. The Contractor shall be responsible for establishing, controlling, maintaining, and ensuring data privacy and an information security program for the Solution in coordination with the TennCare Security and Privacy Offices.
- 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 location.
- A.10.6. The Contractor shall prepare and complete a TennCare System Security Plan (SSP) for the Solution in a format approved by TennCare or directly entered by the Contractor into the TennCare Governance, Risk, and Compliance (GRC) system as directed by TennCare.
- A.10.7. The Contractor shall protect access to Sensitive Data such as Protected Health Information (PHI), Personally Identifiable Information (PII), and Federal Tax Information (FTI) from loss through the design, documentation, development, implementation, operation, and maintenance of security controls over the access to that data in accordance MARS-E (current version) and IRS Pub 1075 (current version).
- A.10.8. The Contractor shall provide evidence to TennCare to validate all security, privacy and encryption requirements contained in MARS-E (current version) and IRS Pub 1075 (current version) are met.
- A.10.9. The Contractor shall comply with MARS-E (current version), IRS Pub 1075 (current version), HIPPA, 42 U.S.C. § 1320d and any applicable State confidentially requirements and standards regarding the collection, maintenance, use, and the protection from data loss of Protected Health Information (PHI) , Personally Identifiable Information (PII) and, Federal Tax Information (FTI).
- A.10.10. The Contractor shall ensure that database security for data at rest and data in motion is in adherence with MARS-E (current version) and IRS publication 1075 (current version).
- A.10.11. The cloud infrastructure for TennCare systems containing Federal Tax Information(FTI) shall be continuously certified as FedRAMP Moderate.
- A.10.12. The Contractor shall employ a data management and data classification strategy and operational policies and procedures that meet HIPAA, MARS-E (current version), IRS Pub 1075 (current version), TennCare policies and procedures and Federal Standards for Security Categorization (FIPS 199) (current version).

- A.10.13. The Contractor shall employ a risk management framework in accordance with TennCare and Federal NIST SP 800-37 (current version) and NIST SP 800-39 (current version) security requirements.
- A.10.14. The Contractor shall ensure all Contractor created policies and procedures adhere to MARS-E (current version) and IRS Pub 1075 (current version) controls for the use of Sensitive Data and separation of duties and shall ensure these documents are made reasonably available for review by TennCare.
- A.10.15. The Contractor shall ensure access to information systems is authorized based on the least privilege principal.
- A.10.16. The Contractor shall maintain and make available at the request of TennCare, policies and procedures for the use of Sensitive Data and separation of duties.
- A.10.17. The Contractor shall develop written policies, procedures, and standards of conduct that articulate the Contractor's commitment 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 Authorized Users, Members, Providers, subcontractors, the Contractor, or external entities.
- A.10.18. The Solution 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 adhere to Federal, State, and TennCare security requirements and shall receive TennCare's approval of its Security Plan.
- A.10.19. The Contractor shall be responsible for identifying and notifying TennCare, within a timeframe that meets TennCare and Federal regulatory requirements, of any Sensitive Data being stored, processed, viewed, or used by the Contractor and all sub-contractors that are in violation of MARS-E (current version) and the TennCare Acceptable Use Policy (AUP) (current version).
- A.10.20. The Solution shall meet password-based authentication and identify requirements in accordance with MARS-E (current version), IRS Pub 1075 (current version), and NIST 800-63-3 (current version).
- A.10.21. The Solution services and infrastructure shall adhere to best practices and use open security standards and frameworks such as, but not limited to:
 - A.10.21.1. Federation: WS-Secure Conversation, WS-Federation, WS-Authorization, XML Key Management (XKMS);
 - A.10.21.2. Mechanism: Extensible Access Control Markup Language (XACML), XML Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML), X.509 certificates; and
 - A.10.21.3. Policy: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL).
- A.10.22. The Solution shall use a security architecture based on the current Medicaid Information Technology Architecture (MITA) Security and Privacy model and Cloud Security Alliance (CSA).
- A.10.23. The Contractor's cloud solution shall be compliant with NIST 800-53 (current version), MARS-E (current version), IRS Pub 1075 (current version) and shall incorporate TennCare required configurations for boundary protection, network segmentation, and access segmentation.
- A.10.24. The Contractor shall perform the installation, operations and management of hardware, application, and operating system level hardening of the solution in accordance with FedRAMP Moderate and CIS Level 1.

- A.10.25. The Contractor shall adhere to Database security in alignment with NIST 800-53 Appendix J (Privacy), CMS Security Center of Excellence guidance, and as directed by TennCare, in accordance with TennCare and federal requirements for all data at rest and in motion.
- A.10.26. 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.10.27. The Contractor shall use synthetic 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.10.28. The Contractor shall meet background check requirements as defined in IRS Pub 1075 (current version) prior to accessing Federal Tax Information (FTI). The Contractor shall maintain a list of employees who have authorized access to FTI. Such list shall be provided to TennCare and, upon request, to the IRS.
- A.10.29. The Contractor shall ensure Federal Tax Information (FTI) shall be used only for the purpose of carrying out the provisions of the contract. The Contractor shall never produce or reproduce FTI in hardcopy. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as shall be necessary in the performance of the contract and pre-approved by TennCare. Inspection or disclosure of FTI to anyone other than those authorized is prohibited.
- A.10.30. The Contractor shall certify that Federal Tax Information (FTI) processed during the performance of the contract shall be completely purged from all physical and electronic data storage in accordance with TennCare data retention policies and with no output retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor shall certify that any FTI in physical or electronic storage shall remain safeguarded to prevent unauthorized disclosures until all is purged.
- A.10.31. The Contractor shall ensure any spoilage that shall result during the processing of Federal Tax Information (FTI) shall be given to TennCare. When this is not possible, the Contractor shall be responsible for the destruction of the spoilage and shall provide TennCare with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- A.10.32. The Contractor shall ensure the solution meets all IRS Publication 1075 (current version) security requirements. To meet the functional and assurance requirements for receiving, processing, storing, or transmitting Federal Tax Information (FTI) the security features of the solution shall provide for the managerial, operational and technical controls to protect the information system against unauthorized use of and access to FTI.
- A.10.33. The Contractor's approved 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.10.34. The Contractor 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.10.35. The Contractor shall ensure data loss prevention and data mining activities are in accordance with MARS-E (current version) and IRS Pub 1075 (current version).

- A.10.36. The Contractor shall ensure solution components run from a service account with access at the level of least privilege. The Contractor shall not run service accounts from a system-level account with unlimited privileges such as "root" or "administrator".
- A.10.37. The Solution 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 MARS-E (current version) and IRS Pub 1075 (current version) requirements.
- A.10.38. The Solution shall integrate with the IAM/ Single Sign-On (SSO) and provide a mechanism for Multi-Factor Authentication (MFA).
- A.10.39. The Contractor shall establish secure connection mechanisms that encrypt data exchanges to access information systems compliant with NIST 800-52 (current version), FIPS 140-3 (or higher), MARS-E (current version), and IRS Pub 1075 (current version).
- A.10.40. The Contractor shall establish and manage cryptographic keys employed within the Solution for key generation, distribution, storage, access, and destruction in accordance with NIST SP 800-175 (current version) and FIPS 140-3 (current version).
- A.10.41. The Solution shall provide a central repository and management platform for security certificates and server host keys.
- A.10.42. Data processed, stored, transmitted and or transported either physically or electronically, within the solutions database, shall be encrypted as required by MARS-E (current version), IRS Pub 1075 (current version), TennCare policies and State and Federal regulations.
- A.10.43. 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.
- A.10.44. The Solution shall provide full redundancy and recovery to ensure uninterrupted access to the certificates and keys.
- A.10.45. The Contractor shall implement a code analysis process in accordance with TennCare Security Standards and Documents.
- A.10.46. The Contractor shall review security and application logs on a regular interval approved by TennCare and no less than as required by MARS-E (current version) and IRS Pub 1075 (current version), to identify suspicious or questionable activity, including fraud and abuse cases, for investigation and documentation as to their cause and remediation.
- A.10.47. 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 Solution, TennCare, or third person's computer, computer system, network, or similar computer-related property and the data, software, and all programs. The Contractor shall implement and manage technical safeguards and physical controls that prevent the unauthorized access to, use of, or tampering with TennCare computer, data or information systems in compliance with MARS-E (current version) and IRS Pub 1075 requirements (current version).
- A.10.48. The Contractor shall coordinate with TennCare to perform security vulnerability scanning and reporting on the Solution and report results through the TennCare ITSM, to include APIs.
- A.10.49. The Contractor shall, twenty-four (24) hours per day, three hundred sixty-five (365) days per year, 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.

- A.10.50. In the event of a breach that compromises or is suspected to compromise the confidentiality, integrity or availability of the solution, the Contractor shall collaborate with the TennCare Security Team to respond to and triage the event. The TennCare Security Team shall be notified of any incident or breach of TennCare in accordance with contract terms and Liquidated Damages.
- A.10.51. The Contractor shall employ application security analysis and testing in accordance with the OWASP Application Security Verification Standard (ASVS).
- A.10.52. The Contractor shall provide TennCare with a use case usage report and review with TennCare on an interval defined and approved by TennCare.
- A.10.53. 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.10.54. The Contractor shall co-manage with TennCare the implementation of a TennCare-owned FIM solution to include the following:
 - A.10.54.1. Install FIM agents across all servers used for the Solution supporting TennCare;
 - A.10.54.2. Provide infrastructure to install FIM collectors in the same network as the Solution;
 - A.10.54.3. Implement capabilities and set up network connectivity to synchronize FIM reports from collector servers to TennCare's centralized FIM; and
 - A.10.54.4. The Contractor shall ensure that the agent's and the collector server's availability meets the SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages.
- A.10.55. All State owned/supported workstations shall be managed by STS using established State-standard software tools.
- A.10.56. The Contractor shall install and configure TennCare-approved antivirus solutions across all servers used for the Solution and make the findings available in a format and frequency as requested by TennCare.
- A.10.57. 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.10.57.1. Antivirus and antispyware;
 - A.10.57.2. Host firewall;
 - A.10.57.3. Host intrusion prevention system;
 - A.10.57.4. Host integrity check; and
 - A.10.57.5. Application device control.
- A.10.58. The Contractor, on approval by TennCare, shall configure, develop, implement, operate, and manage endpoint security capabilities in accordance with MARS-E (current version) and IRS Pub 1075 (current version) and shall schedule scans to continuously protect TennCare information systems from malware, ransomware, persistent threats, and data-loss attack activities monitored in real-time.

- A.10.59. The Contractor shall provide TennCare with all endpoint protection security enforcement rules and policy definitions upon request and grant Read-Only access to the endpoint protection manager portal at all times.
- A.10.60. The Contractor shall enable appropriate logging mechanisms on systems and applications to monitor all user access activities, authorized and failed access attempts, system exceptions, and critical information security events in accordance with MARS-E (current version) and IRS Pub 1075 (current version).
- A.10.61. The Solution shall integrate with TennCare's Security Information and Event Management (SIEM) solution in accordance with the IRS SIEM tool standards. This standard is to be used for all data classifications.
- A.10.62. The Contractor shall implement audit mechanisms to generate findings and reports across different layers of the solution in accordance with FedRAMP (current version), MARS-E(current version) and IRS Pub 1075 (current version).
- A.10.63. The Contractor shall ensure the configuration of secure log data and event collection mechanisms is in accordance with MARS-E (current version) and IRS Pub 1075 (current version) and deliver to TennCare for indexing and analysis at a frequency determined by TennCare. This includes, at a minimum, the end-to-end process from log data collection, event generation, transmission, storage, and disposal.
- A.10.64. The Contractor shall ensure the Solution retains security, application, system audit, and event logs per MARS-E (current version) and TennCare retention requirements (current version) and in a format and structure that is approved by TennCare.
- A.10.65. The Contractor shall provide TennCare access to the Solution log and event data for review or extraction 24-hours a day, 7 days a week, 365 days a year. The Solution shall be capable of creating a digital, reusable copy of TennCare's data, in whole or parts in common and current machine-readable files. TennCare shall be able to extract TennCare's data from the solution on-demand within a reasonable amount of time which shall not exceed twenty-four (24) hours following a TennCare request. Said data shall be provided by the Contractor without charge and without condition or contingencies.
- A.10.66. The Contractor shall participate in audit activities and assist TennCare to prepare documentation required by TennCare and/or any regulatory bodies.
- A.10.67. The Contractor shall have an annual audit performed by a qualified, third-party, independent audit assessor (Assessor), approved by TennCare, who shall conduct an assessment of the security and privacy controls in the solution. A Security Assessment Plan (SAP) shall be jointly completed and agreed to prior to the start of the assessment by the Contractor, the Assessor, and TennCare. The Assessor shall use the methodology described in the template provided by TennCare to complete the SAP. A completed SAP shall be submitted to TennCare 70 days prior to the security assessment kick-off date. The full un-redacted third party independent assessment shall be delivered to TennCare on demand within 10 business days upon receipt of the report from the Assessor.
- A.10.68. The Solution shall have the ability to identify and alert on any application layer Distributed Denial of Service (DDoS) attacks.
- A.10.69. 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 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.
- A.10.70. The Contractor shall provide evidence to TennCare to validate all security, privacy and encryption requirements contained in MARS-E (current version) and IRS Pub 1075 (current version) are met.

- A.10.71. The Contractor shall provide TennCare with written evidence of findings (defects, vulnerabilities, errors, gaps, weaknesses and omissions) and their planned remediation in a Plan of Action and Milestone report (POA&M), maintained monthly, until all findings are resolved.
- A.10.72. The Contractor shall, within 30 days of a discovered finding, create and provide TennCare with written evidence of findings (defects, vulnerabilities, errors, gaps, weaknesses and omissions) and their planned remediation in a Plan of Action and Milestone report (POA&M) and shall present monthly until all findings are resolved.
- A.10.73. The Solution shall track disclosures of PHI and PII and provide Authorized Users access to and reports on the disclosures. These disclosure reports shall be provided to TennCare within the time limits mandated per the TennCare Privacy Program Policy and Plan.
- A.10.74. The Contractor shall develop, maintain, and test an Incident Response Plan (IRP), included in the Incident Management Plan, with key partner roles both internal and external on an annual basis in accordance to the NIST SP 800-61 (current version) and comply with all applicable Federal, State and TennCare breach notification laws and policies. The Contractor shall create and submit compliance and regulatory reports in accordance with Federal, State, and TennCare requirements regarding security-related events and incidents while working with TennCare towards security recovery actions.
- A.10.75. The Contractor shall notify the TennCare Security and Privacy Offices within ten (10) Business Days of any Solution or operational enhancements, Control 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.10.76. The Contractor shall be responsible for the continuity of all security and privacy protocols for all Solution material changes contained in Change Memorandums related to key deliverables within the Security and Privacy development cycles. The Contractor shall notify by written email to the TennCare Security and Privacy Offices upon agreement of solution or operational enhancements, Control Memorandums, or materials changes.
- A.10.77. The Solution shall utilize the TennCare-provided IAM solution for TennCare staff and shall provide role-based security for the identity management and authentication of TennCare end-users. 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.10.78. The Solution shall provide an access and privileging solution for Authorized User(s) and shall provide role-based security for the identity management and authentication of individuals.

A.11. Solution Implementation Lifecycle (SILC) Standard Requirements

- A.11.1. The Contractor shall follow the TennCare's Solution Implementation Lifecycle (SILC) Standard located in Attachment C, Procurement Library. The TennCare Solution Implementation Lifecycle Standard 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 Standard and defined in the CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables located in Attachment C, Procurement Library. The CLRS 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 in the "DDI Phase I" and "DDI Phase 2" tabs of the CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix A of the TennCare Solution Implementation Lifecycle Standard for role definitions) for the DDI of the Solution.
 - 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 CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables. If the Deliverable does not have a defined Business Review Cycle in column I 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 in the "O&M Phase 1" and "Solution O&M" tab of the CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix A of the TennCare Solution Implementation Lifecycle Standard for role definitions) for O&M of the Solution.
 - 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 CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables. If the Deliverable does not have a defined Review Cycle in column I 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 Standard, 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 Solution 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 online hyperlinks with references to Medicaid and non-Medicaid policy origination documents managed by TennCare and the Contractor within the project document library.
- A.11.6.5. 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.11.6.6. The Contractor shall categorize documentation by data classification, as defined by TennCare, and securely store sensitive technical documentation as approved by TennCare.
- A.11.6.7. 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 the TennCare Project Management Plan Standard located in the Attachment C, Procurement Library.
- 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 submission of the original Deliverable 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 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.14.), 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 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, and CMS Certification, as required by any local, State, or federal entities for the Solution throughout the duration of the Contract.
- A.11.8.2. The Contractor shall be responsible for adherence to the established TennCare Integration Standards during implementation of the Solution.
- A.11.8.3. 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.11.8.3.1. 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 requirements contained in 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 TennCare to plan, prepare for, execute, and report on testing.
 - A.11.9.2.2. The Contractor shall prepare a Test Management Plan for the Solution 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:
 - A.11.9.2.4.1. Unit Test Report;

- A.11.9.2.4.2. System Integration Test Report;
- A.11.9.2.4.3. User Acceptance Test (UAT) Report;
- A.11.9.2.4.4. Operational Readiness Test (ORT) Report; and
- A.11.9.2.4.5. 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 TennCare Test Management Standard, located in Attachment C, Procurement Library.
- 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 TennCare 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 TennCare Contractor(s) for all phases of testing as defined in the TennCare Solution Implementation Lifecycle Standard.
- A.11.9.2.9. The Contractor shall participate in and support User Acceptance Testing (UAT) for Configuration Items (CI) 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 TennCare Contractor(s) 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") located in the TennCare Test Management Standard in Attachment C, Procurement Library.

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 Solution in the approved SOP Manual.
- A.11.10.1.3. The Contractor shall build and maintain a delimited SOP Manual for the Solution for the purposes of easily onboarding new resources and consistent operation of the Solution. 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 Manual as the document of record for Solution activities, maintain the SOP Manual under Configuration Management control, and update SOP Manual 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 a staffed Module Support Team during normal business hours for production support to coordinate service issue identification, investigation, and diagnosis in cooperation with TennCare, the IS Contractor, and TennCare Contractor(s). Communication channels for support shall include email and phone among other channels offered by the Contractor. Normal business hours are defined as 7:00 AM to 9:00 PM Central, Monday through Friday, excluding State observed holidays. The Contractor shall not be responsible for the support activities of other TennCare Contractors' Module Support Teams.
- A.11.10.2.2. 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.
- A.11.10.2.3. The Contractor shall utilize the TennCare-approved ITSM tool to provide Module Support services for the Solution and record and manage service-related activities.
- A.11.10.2.4. The Contractor shall manage and track all Solution-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.11.10.2.5. 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 IT Service Management Standard for the Service Desk function.
 - A.11.10.2.5.1. 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 Module Support Team.
- A.11.10.2.6. The Contractor shall provide Tier II Level Support, consisting of support services that require technical resources who have specialized skills related to the Solution.
- A.11.10.2.7. The Contractor shall provide Tier III Level Support requiring technical expertise related to the Solution.
- A.11.10.2.8. 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 MMPVP of CI(s) changes that impact TennCare activities.

- A.11.10.2.9. The Contractor shall be responsible for reporting the resolution results to the Tier I Service Desk.
- A.11.10.2.10. The Contractor shall develop an incident priority matrix for Module Support Team Incident Management activities subject to TennCare approval.
- A.11.10.2.11. 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 MMPVP.
- A.11.10.2.12. The Contractor shall integrate Contractor's 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.11.10.2.13. The Contractor shall provide reoccurring status updates on GRC activities in coordination with the IS Contractor on a timeline defined by TennCare.
- A.11.10.2.14. The Contractor shall monitor the production environment twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year and develop, maintain, and manage a plan to monitor every operation that affects the Solution and associated CIs (e.g., network, software, interfaces, services, data manipulation).

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 Solution technology components.
- A.11.10.3.2. The Contractor's IT Operations Management shall have the capability to intake requests from the IS Contractor's Tier I Service Desk via the TennCare ITSM tool from internal and external Stakeholders interacting with the Solution.
- A.11.10.3.3. The Contractor shall integrate the Solution 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 Solution 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 IS Contractor's enforcement activities for Solution 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 Solution.
- A.11.10.3.8. The Contractor shall maintain compliance with the SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages.

A.11.10.4. Technical Management

- A.11.10.4.1. The Contractor shall be responsible for the technical management function of the Solution, providing technical skills and capabilities in support of TennCare services, and management of the Solution. 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 Solution to include, at a minimum, the following activities:
 - A.11.10.4.2.1. Operating system support;
 - A.11.10.4.2.2. License management;
 - A.11.10.4.2.3. Third-level support;
 - A.11.10.4.2.4. Application management;
 - A.11.10.4.2.5. Procurement advice;
 - A.11.10.4.2.6. System security;
 - A.11.10.4.2.7. Definition and management of virtual servers;
 - A.11.10.4.2.8. Assistance to capacity management;
 - A.11.10.4.2.9. Ongoing maintenance; and
 - A.11.10.4.2.10. 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 directory services activities to ensure process information about IT infrastructure is available online with appropriate user access rights as defined by the State.
- 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 State's VPN 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 Solution-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 MMPVP to ensure alignment with TennCare's enterprise architecture and required levels of availability required by TennCare.
- A.11.10.5.3. The Contractor shall organize the Solution 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 Solution 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 CIP to include repeatable, defined, and efficient management processes for optimization of Solution-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) located in the Attachment C, Procurement Library, and is approved by TennCare.
- A.11.10.6.5. The Contractor shall 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 the Solution to improve the services across the enterprise and enhance service offerings to Members and individuals.
- 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 Solution 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 MMPVP in alignment with TennCare priorities and goals.
- A.11.10.7.2. The Contractor shall monitor patterns of Solution 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 Authorized Users.
- A.11.10.8.1.2. The Contractor shall coordinate with the IS Contractor on Solution 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 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.11.10.8.1.6. 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 TennCare IT Service Management 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 Catalog and Service Portfolio.
 - A.11.10.8.2.4. The Contractor shall manage the Solution Service Catalog under formal Change Management control.
 - A.11.10.8.2.5. The Contractor shall provide TennCare the necessary inputs for Medicaid Modernization Program (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 MMPVP 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 Solution, and support TennCare in the drafting of future SLA documentation in coordination with TennCare-identified Contractor partners.
 - A.11.10.8.2.9. The Contractor shall conduct review meetings with TennCare and MMPVP and produce standard reports to review the service achievement for TennCare and MMPVP 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 Solution 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 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 Solution Implementation Lifecycle Standard and defined in the CLRS TennCare Solution Implementation Lifecycle 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 CIP 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 Solution.
 - 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 Solution 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 Solution.
 - 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 Solution-related systems, which include production and non-production environments (e.g., development, test, training). 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 Solution 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., CPU, 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 MMPVP 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, and underpinning service agreements/contracts and criteria, for a standardized approach for Solution availability management for TennCare approval.
- A.11.10.8.4.2. The Contractor shall be responsible for monitoring availability data for the Solution.
- 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 Solution.
- A.11.10.8.4.4. The Contractor shall use simulation, modeling, and load test tools in order to ensure that the Solution 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 Solution 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 Solution 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 Solution 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 shall have a complete understanding of TennCare Security Requirements Standards and Documents.
- 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 TennCare 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 Solution performance issues and improvement opportunities.
- A.11.10.8.7.2. The Contractor shall analyze the performance data of the Solution 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 the Solution to resolution and providing relevant documentation to TennCare.
- A.11.10.8.7.4. The Contractor shall support TennCare, IS Contractor, and MMPVP in the design and implementation of a high-performance Solution to achieve and exceed minimum acceptable service levels based upon the performance management analysis requirements in this Section.
- 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 Solutions 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 Solution.
- A.11.10.9.1.4. The Contractor shall coordinate change, build, and test activities for the Solution.
- A.11.10.9.1.5. The Contractor's Change Management process shall include procedures to authorize change deployment for the Solution 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 promote transparency and visibility to the Solution.

- 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 processes applicable to Change Evaluation in coordination with the IS Contractor, including the TennCare IT Service Management Standard located in Attachment C, Procurement Library.
- 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 Solution and Authorized 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) included in the Operations & Maintenance Run Book.
- A.11.10.9.3.2. The Contractor shall adhere to TennCare policies including, but not limited to, applicable TennCare policies located in Attachment C, Procurement Library, regarding 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 Solution.

- 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 Solution for TennCare approval.
- A.11.10.9.3.5. The Contractor shall be responsible for coordination of all 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 monitoring and reporting progress on Service Transitions to include, at a minimum:
 - i. Transition status updates;
 - ii. Configuration compliance reviews; and
 - iii. Evaluation reports.
- A.11.10.9.3.7. The Contractor shall contribute to IS Contractor Service Transition activities as defined 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 the Solution potential deployments and developing concrete deployment plans in coordination with the IS Contractor and MMPVP.
 - 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 CIs and components, release packaging content, and procedures for the building and management of the test environments. These procedures should be 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, address:
 - i. Deployed processes;
 - ii. Transfer/deployed service;
 - iii. Decommissioning and service retirement;
 - iv. Removal redundant assets; and
 - v. Assessments of completed deployment.

- A.11.10.9.4.7. 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 MMPVP and incorporating industry-standard continuous integration and deployment approaches for cloud environments to ensure all parties are ready for releases.
- A.11.10.9.4.8. The Contractor shall provide technical release notes in advance of each release.
- A.11.10.9.4.9. The Contractor shall ensure that all code releases follow best practices for separation of duties (e.g., developers should never deploy code).
- A.11.10.9.4.10. The Contractor shall perform all deployments other than emergency releases during non-business hours.
- A.11.10.9.4.11. The Contractor shall coordinate all releases with the IS Contractor and relevant MMPVP to avoid any potential adverse impacts on the Solution 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 Solution in coordination with the IS Contractor and MMPVP.
 - 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 Solution in coordination with the IS Contractor and MMPVP.
 - A.11.10.9.5.4. The Contractor shall be responsible for preparing test environments for the Solution in coordination with the IS Contractor and MMPVP.
 - A.11.10.9.5.5. The Contractor shall be responsible for development of supplemental test cases for testing activities for the Solution in coordination with the IS Contractor and MMPVP.
 - A.11.10.9.5.6. The Contractor shall be responsible for evaluating testing exit criteria for the Solution in coordination with the IS Contractor and MMPVP.
- 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, including, but not limited to, Configuration Management and planning, Configuration Item identification, Configuration Item control, status accounting and report, and verification and accounting.
 - 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 Solution.
- 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 Knowledge Management strategy for TennCare approval and alignment of the Solution 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, including, but not limited to, defining Knowledge Management strategy, identify and gather data sources, draft knowledge, technical review, editorial review, and publish.
- A.11.10.9.7.4. The Contractor shall be responsible for coordinating Solution 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 and maintenance of the Solution data and information requirements and associated information architecture definitions.
- A.11.10.9.7.6. The Contractor shall be responsible for establishing the Solution 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 management of Solution Event detection.

- A.11.10.10.1.2. The Contractor shall be responsible for correlating and filtering events and routing or receiving event-related information, as appropriate.
- A.11.10.10.1.3. The Contractor shall be responsible for ensuring that the Solution is designed to support Event Management.
- A.11.10.10.1.4. The Contractor shall be responsible for categorization of events in alignment with the TennCare Integration Standard.
- A.11.10.10.1.5. The Contractor shall be responsible for reviewing the events that have been resolved appropriately as defined by TennCare.
- A.11.10.10.1.6. 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 Solution 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 Solution, including, but not limited to, incident registration and categorization, prioritization, investigation and diagnosis, resolution, and closure.
- A.11.10.10.2.3. The Contractor shall be responsible for management of the Solution incident prioritization activities.
- A.11.10.10.2.4. The Contractor shall be responsible for management of the Solution incident investigation and diagnosis.
- A.11.10.10.2.5. The Contractor shall be responsible for management of the Solution incident resolution and closure.
- A.11.10.10.2.6. The Contractor shall be responsible for providing a consolidated view of the Solution, to include Event Management and Incident Management along with other appropriate processes that shall enable TennCare and the IS Contractor to have full visibility of the Solution.

A.11.10.10.3. Request Fulfillment Management

- A.11.10.10.3.1. The Contractor shall be responsible for request registration, i.e. request initiation and validation, for Solution 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 policies including, but not limited to, applicable TennCare policies located in Attachment C, Procurement Library, or the Solution Request Fulfillment activities.
- A.11.10.10.3.4. The Contractor shall be responsible for validating the Solution 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 of service requests.
- A.11.10.10.3.7. The Contractor shall be responsible for closure of the Solution service requests.

A.11.10.10.4. Access Management

- A.11.10.10.4.1. The Contractor shall support TennCare and IS Contractor activities regarding coordination and support of access management activities, including, but no limited to, access requisition, verification and validation, provision of rights, monitoring the access, tracking the access, and de-provisioning the access.
- A.11.10.10.4.2. The Contractor shall be responsible for management of the Solution access verification and validation of requisition activities.
- A.11.10.10.4.3. The Contractor shall be responsible for monitoring, tracking, and controlling the access to the Solution.
- A.11.10.10.4.4. The Contractor shall be responsible for de-provisioning access for Authorized Users and the Solution.

A.11.10.10.5. Problem Management

- A.11.10.10.5.1. The Contractor shall be responsible for Solution 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, including, but no limited to, Problem detection and logging, categorization, investigation and diagnosis, and resolution and closure of Problem.
- 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 Solution. These procedures shall include precise steps for investigation, diagnosis, resolution, and closure of Problems. These procedures shall be included in the SOP.

A.11.10.11. Turnover

- A.11.10.11.1. If applicable, the Contractor shall cooperate with TennCare in transitioning the Solution and responsibilities of this Contract to TennCare, authorized contractor, and/or successor contractor upon termination or expiration of this Contract.
- A.11.10.11.2. 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.11.10.11.3. The Contractor shall ensure that a Turnover Plan, as defined in the TennCare Solution Implementation Lifecycle Standard, 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.11.10.11.3.1. A timeline with milestones for the Turnover to include planning, execution, and implementation approval;
- A.11.10.11.3.2. Description of maintenance process for Turnover documentation and Artifacts throughout the life of the Contract; and
- A.11.10.11.3.3. Any additional information requested by TennCare in a CM.
- A.11.10.11.4. 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.11.10.11.4.1. Security profiles of the platform Authorized Users and service accounts in a Microsoft Word document or Microsoft Excel spreadsheet format; and
 - A.11.10.11.4.2. 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.11.10.11.5. The Contractor shall provide post-Turnover support for up to one hundred twenty (120) calendar days, including Deliverables and associated activities specified in a CM and agreed to by TennCare.
- A.11.10.11.6. The Contractor shall complete financial reconciliation of this Contract, including liquidated or financial consequences, if applicable.
- A.11.10.11.7. 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. TennCare requires the Solution to be certified by CMS back to Day 1 of the Operations and Maintenance Phase. The Contractor 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 Solution 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 Standard. 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 address and satisfy all CMS documentation requirements for EFPF throughout the Term of the Contract, as well as requests for information and/or documentation, with the approval of TennCare.
- A.12.1.3. The Contractor shall collaborate with TennCare to provide a Certification Plan, as defined in the TennCare Solution Implementation Lifecycle Standard, 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.12.1.4. The Contractor shall develop a Certification Crosswalk that describes how the Contractor's evidence Artifacts, Deliverables, and other control documentation align with Federal certification requirements, evaluation criteria, milestone reviews, and reporting.
- A.12.1.5. The Contractor shall support CMS Certification for the Solution. 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, providing support during the actual certification milestone review meeting, and providing a demo and expertise, as defined in the TennCare Solution Implementation Lifecycle Standard and CMS' certification requirements.
- A.12.1.6. Prior to Go-Live of the Solution, the Contractor shall engage a TennCare-approved outside party to conduct a Third-Party Security and Privacy Assessment, as defined in the TennCare Solution Implementation Lifecycle Standard, 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 shall be available for review by TennCare, CMS, and MMPVP. Additional reports required by CMS will be provided at no additional cost to TennCare. The Contractor shall also 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.12.1.7. The Contractor shall integrate the certification timeline and tasks into the Contractor's project schedule. The Contractor shall provide in the project schedule all certification related tasks and timelines. Prior to the Go-Live date, as defined in project schedule, the Solution 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 Solution Artifacts and documentation that CMS requires. Following the Go-Live date as defined in project schedule, the Solution will be evaluated for certification by CMS using the agreed upon version of the certification requirements. CMS requires the 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.
- A.12.1.8. At no additional cost to TennCare, the Contractor shall participate and provide support as needed to the Solution for module certification activities including participating in planning activities, meetings, ongoing reporting efforts, and other activities as required by CMS.
- A.12.1.9. The Contractor shall provide a Certification Manager, as defined in the table in Section A.12.3.5., to collaborate and coordinate with TennCare and the MMPVP 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.12.1.10. The Contractor shall create and/or update system, user, and training documentation as necessary to support the certification process and to reflect changes that have been made to the Solution during the certification process.

A.12.2. Staffing

A.12.2.1. General Staffing Requirements

- A.12.2.1.1. All personnel shall be employees or subcontractors of the Contractor and fully qualified to perform the work required in this Contract. The Contractor shall provide experienced, qualified professionals to be engaged with TennCare. The Contractor shall provide personnel in sufficient quantity to meet all requirements of the Contract.
- A.12.2.1.2. The Contractor's work will normally occur during TennCare's Business Days, 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. The Contractor shall furnish Contractor personnel as needed for after-hours projects. The Contractor's work and travel schedules shall be approved in advance by TennCare's Program Director or their designee.
- A.12.2.1.3. Other than required approval of Key Personnel and subcontractors by TennCare as detailed in A.12.3., 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 Solution and anticipated future needs for the Solution. TennCare will use the CM process to indicate dates by which staffing increases or replacements must be made. Failure to meet the staffing deadlines in the CM may lead to the imposition of Liquidated Damages as specified in Attachment B, Service Level Agreements and Liquidated Damages.
- A.12.2.1.4. On-Site Staffing Requirements. Personnel are considered On-Site when working at either the Contractor's offices described in Section A.12.4. or at the TennCare offices located in Nashville, Tennessee.
- A.12.2.1.5. The Contractor shall ensure that the roles that are established and staffed to support O&M are included in the measurement of O&M headcount for a given period, even though they may also be supporting enhancement activity for the same period.
- A.12.2.1.6. 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.12.2.1.7. 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.

A.12.2.2. Subcontractor Staff

- A.12.2.2.1. With regard to those subcontractors approved by TennCare 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.

- A.12.2.2.2. 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. Key Personnel

A.12.3.1. General Requirements

- A.12.3.1.1. Key Personnel are Contractor personnel deemed by TennCare to be essential to the Contractor's satisfactory performance of the requirements contained in this Contract, in Section A.12.3.5. Table – Key Personnel contains the required Key Personnel positions, corresponding roles and responsibilities, and minimum qualifications for each.
- A.12.3.1.2. The Contractor shall obtain TennCare's prior written approval of all Key Personnel. The Contractor shall provide resumes for all Key Personnel to 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 person 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.12.3.1.3. If the Contractor deems an additional Key Personnel position(s) necessary beyond the positions listed in Table 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 committed in writing to join the project by the beginning of the Contract Effective Date.
- A.12.3.1.4. If any Key Personnel are not employees of the Contractor, the Contractor shall identify those personnel and provide TennCare with contracts establishing the Key Personnel's subcontract. The Contractor shall not employ or use a subcontractor without the approval of TennCare.
- A.12.3.1.5. References for Key Personnel shall meet the following requirements:
- A.12.3.1.5.1. A minimum of three (3) professional references who can provide information about the Key Personnel's work on relevant past assignments as outlined in A.12.3.1.6.4.;
 - A.12.3.1.5.2. The reference's full name, mailing address, telephone number, and e-mail address;
 - A.12.3.1.5.3. 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; and
 - A.12.3.1.5.4. The Key Personnel's professional experience within the past five (5) years.

- A.12.3.1.6. Key Personnel resumes shall include the following information:
 - A.12.3.1.6.1. Employment history for all relevant and related experience;
 - A.12.3.1.6.2. Names of employers for the past five (5) years, including specific dates;
 - A.12.3.1.6.3. All educational institutions attended, and degrees obtained; and
 - A.12.3.1.6.4. All professional certifications and affiliations.
- A.12.3.1.7. 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.12.3.1.8. 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. In the event it becomes necessary to replace Key Personnel during the term of this Contract, the Contractor shall:
 - A.12.3.1.8.1. 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.12.3.1.8.2. Provide TennCare's Program Director with documentation describing the circumstances of the need for the replacement;
 - A.12.3.1.8.3. Provide documentation of experience for the proposed replacement personnel;
 - A.12.3.1.8.4. Obtain prior written approval from TennCare's Program Director; and
 - A.12.3.1.8.5. 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 Attachment B, Service Level Agreements and Liquidated Damages.

A.12.3.2. Staffing Needs Planning and Monitoring Processes

- A.12.3.2.1. 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.12.3.3. Turnover Staffing

- A.12.3.3.1. The Contractor shall provide a full-time Turnover manager one-hundred eighty (180) calendar days prior to the end of the Contract Term as a designated point person to interact with TennCare and a successor contractor until Contract Term is completed.
- A.12.3.3.2. The Contractor shall provide and retain sufficient Key Personnel 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.12.3.3.3. The Contractor shall include staffing for operations during Turnover in the Turnover Plan.

A.12.3.4. Off-Boarding

- A.12.3.4.1. 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.12.3.4.2. In the event of a Key Personnel 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 Key Personnel submits their resignation.

A.12.3.5. Key Personnel Table

Key Personnel	Description	Minimum Qualification	Requirements
Account Director	The Account Director shall have day-to-day authority to manage all Contract requirements and the Contractor's services for the Solution. The Account Director shall also serve as the primary point of contact for all activities related to contract administration, project management, scheduling, resource management, correspondence with TennCare's Leadership, and deliverable reviews.	• A minimum of ten (10) 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, including operations and maintenance. • A minimum of five (5) years of experience serving in an account management or client representative position. • Subject Matter Professional (SMP) on relevant State and Federal Medicaid regulations and policies. • 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 Key Personnel position. • Shall be available for the entire term of the Contract and is expected to contribute at least 10% of annual Full-Time Equivalent (FTE) support to the specified role on the project.
Project Manager	The Project Manager shall be responsible for all planning, directing, managing, and overseeing the overall CLRS Contractor Project Management activities.	• A minimum of eight (8) years of experience managing IT systems programs and/or projects similar to the Solution. • 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. • Required Project Management Professional (PMP) certification.	• Shall be available as needed throughout the term of the Contract.

Technical Subject Matter Professional (SMP)	The Technical SMP shall serve as a single technical point of contact with TennCare's Information Systems (IS) staff. The Technical SMP shall lead the development and implementation for the end-to-end Solution by taking into consideration TennCare's business case, objectives, requirements, constraints, technology landscape, technology standards, and cloud hosting requirements.	• A minimum of eight (8) years of experience implementing large-scale healthcare IT solutions within environments similar to that of the CLRS. • A minimum of eight (8) years of experience building and supporting multi-tier large scale healthcare applications. • A minimum of five (5) years of experience in cloud infrastructure and systems design. • A minimum of five (5) years of direct experience configuring, operating and maintaining cloud environments. • Expert knowledge of the Contractor's Solution, having implemented a solution in no less than one (1) environment at least as complex as the TennCare environment. • Shall be familiar with Data Governance concepts like Metadata Management and Master / Reference Data Management. • Extensive experience utilizing Service-Oriented Architecture (SOA) patterns, automating business process models and employing cloud based services • Extensive experience architecting multi-tier platforms that employ SOA. • Shall be knowledgeable of secure coding practices. • Experience with Medicaid Information Technology Architecture (MITA). • Experience with technical requirements for data classifications and implementing data protection technologies. • Extensive experience developing solutions utilizing an integrated development environment, multi-tier platforms and employing SOA architecture with high availability/reliability requirements.	• Shall not serve in any other Key Personnel position. • Shall be available for the entire term of the Contract and is expected to contribute at least 75% of annual FTE support to the specified role on the project.
--	--	---	---

		• Must be proficient in multiple languages, SOA technologies, operating systems and security best practices. • Experience implementing data warehouse solutions within an integrated environment and employing SOA and intelligent business reporting. • 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, Domain Name System (DNS) and Certificates. • Knowledge of complex network routing.	
CLRS Solution Manager	The CLRS Solution Manager shall be responsible for overseeing the detailed Solution requirements activities, Solution design and development, and Solution readiness activities throughout the relevant phases of the TennCare SILC. The CLRS Solution Manager shall manage technical resources and Solution functionality throughout the project lifecycle. The CLRS Solution Manager shall be responsible for oversight and management of all Solution requirements throughout the operations and maintenance phases. This shall include maintaining all relevant hardware, software, and Artifacts in accordance with requirements and TennCare Standards.	• Possess expert knowledge of the Contractor's CLRS, having implemented an CLRS solution in no less than one (1) environment at least as complex as the TennCare environment. • 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. • A minimum of seven (7) years of experience on technical aspects of solutions including, but not limited to, infrastructure, application, and data warehousing. • A minimum of five (5) years of similar O&M management experience. • Extensive experience architecting multi-tier platforms that employ SOA. • Extensive experience utilizing SOA patterns, automating business process models and employing cloud-based services. • Shall be familiar with multiple	• Shall not serve in any other position during the DDI and O&M Phases. • Shall be available for the entire term of the Contract and is expected to contribute at least 75% of annual FTE support to the specified role on the project.

		integration methods, SOA technologies, and industry relevant security standards. • Previous experience in maintaining and adhering to Service Level Agreement requirements.	
Testing Manager	The Testing Manager shall perform and provide technical leadership for test activities to include planning, execution, and reporting of the CLRS. The Testing Manager shall work with TennCare and designated Contractor partners throughout the testing process and shall adhere to and be responsible for implementing the activities outlined within the TennCare Test Management Standard.	• A minimum of eight (8) years of experience in managing testing functionalities similar to the CLRS. • Demonstrated experience and knowledge of Industry Standard and best practices regarding large-scale and enterprise- level projects. • A minimum of five (5) years of experience performing similar services on cloud based applications/systems with emerging and modern technology. • Demonstrated experience in technical writing. • Preferred experience in healthcare related concepts. • A minimum of five (5) years of experience analyzing requirements and designing/executing test strategies, test plans, and test cases using an Industry Standard test management tool. • One (1) or more full lifecycle engagements as a test lead/manager for the proposed solution or product, or for a solution of similar scope.	• Shall be available as needed throughout the term of the Contract.

Certification Manager	The Certification Manager shall be the primary contact for TennCare with its engagement and interaction with Centers for Medicare & Medicaid (CMS) for certification efforts of the CLRS. The Certification Manager shall also ensure that system functionality and business operations meet the CMS Certification criteria as specified by CMS throughout the term of the contract. The Certification Manager shall develop and implement a strategy and plan for proper documentation of system artifacts to support the certification process.	• A minimum of five (5) years of similar CMS Certification experience.	• Shall be available as needed throughout the term of the Contract.
Training Manager	The Training Manager shall provide internal training to Authorized Users on the Solution components and functionality of the CLRS. The Training Manager shall also oversee production of any publications and materials for Authorized Users, to include desk aides, video resource trainings, and online help documentation creation.	• A minimum of five (5) years of experience in managing training of on an IT solution similar in scale to the CLRS. • Demonstrated experience and knowledge of industry standard and best practices regarding large-scale and enterprise-level projects. • A minimum of three (3) years of experience performing similar services on cloud based applications/systems with emerging and modern technology. • Extensive experience in technical writing. • Preferred experience in healthcare related concepts, such as Health Starts Initiative, Care System Redesign, and Health Change Management.	• Shall be available as needed throughout the term of the Contract.
Data Analytics Manager	The Data Analytics Manager shall lead the strategy and implementation for the reporting architecture components of the CLRS by taking into consideration TennCare's business case, objectives, requirements, and constraints. The Data Analytics Manager shall also be	• A minimum of five (5) years of experience in data analytics reporting. • A minimum of three (3) years of experience leading and managing a data analytics team. • Expert knowledge in Dashboard configurations.	• Shall be available as needed throughout the term of the Contract.

	responsible for the technical domain which includes conceptual, logical, and physical data modeling, information delivery standards, best practices, tools and technologies, security in the information delivery environment, information delivery architecture, design, development, capacity planning, performance tuning, and administration.	• Significant experience managing Federal and State reporting requirements. • Extensive experience dealing with Sensitive Data, and healthcare Industry Standards and regulations. • Technical understanding and expertise in enterprise data modeling and programming. • Willingness to question the validity, accuracy of data and assumptions. • Working knowledge of Structured Query Language (SQL), Python, Snowflake, or other Database functional knowledge.	
Security Subject Matter Professional (SMP)	The Security SMP shall be responsible for the assessment, planning, and implementation of all security standards, practices, and components required for the CLRS implementation. The Security SMP shall also be responsible for adherence to TennCare security standards, communications with TennCare Security and Privacy Officer compliance with HIPAA, Health Information Technology for Economic and Clinical Health (HITECH) and National Institute of Standards and Technology (NIST) requirements, and Internal Revenue Service (IRS) Federal Tax Information.	• A minimum of eight (8) years related experience in a large scale environment similar to the CLRS. • Must be familiar with at least one 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 project with similar size and scope. • At least one (1) relevant professional information security certification required: CISSP, CISM, CRISC, SANS, GIAC, or similar. • Extensive experience dealing with Sensitive Data information systems.	• Shall be available as needed throughout the term of the Contract.

Project Scheduler	The Project Scheduler shall work directly with the TennCare Project Management Office (PMO), Strategic Project Management Office (SPMO), and the Contractor's PMO to ensure that the CLRS schedule is developed, updated, and maintained in alignment with the cadence and process established for the program.	• Extensive experience in developing and maintaining project timelines for large scale IT solutions. • Experience following a standard project management methodology and using various project management tools in developing project plans, delivering tasks, and tracking timelines and resources. • Working knowledge of Project Scheduling software such as Microsoft Project 2013 (or later), Microsoft Project Server, and Microsoft Excel. • Preferred PMP Certification.	• Shall be available as needed throughout the term of the Contract.
State Resource Manager	The State Resource Manager shall oversee the Regional Resource Liaisons during CBO recruitment, training, and retention throughout the state. The State Resource Manager shall serve as the primary point of contact for the requirements outlined supporting the Community Resource Directory and shall oversee routine updates to the Community Resource Directory. The State Resource Manager shall develop a strategic framework for expanding engagement of new CBOs to utilize the Solution, including expanding the number of Verified CBO Service Location(s) and Active CBO Service Location(s). The State Resource Manager shall oversee all external and internal customer service management related to the Community Resource Directory.	• A minimum of five (5) years of experience working with CBOs mission-focused on delivering basic needs/human service supports, including but not limited to housing, food, transportation, workforce, utility, or other related Domains. • A minimum of five (5) years of experience working with Tennessee CBOs with an approximate annual budget at or above \$3.5 million. • Strong understanding of safety net programs available in Tennessee. • Extensive experience in managing recruitment, training, and retention efforts of MCOs, Providers, and CBOs for an IT solution similar in scale to the CLRS. • Extensive experience in customer service management for a IT solution similar in scale to the CLRS.	• Shall be available for the entire term of the Contract and is expected to contribute at least 75% of annual Full-Time Equivalent (FTE) support to the specified role on the project.

Regional Resource Liaisons	A minimum of three (3) Regional Resource Liaisons shall perform recruitment, training, and retention activities for CBO partnerships throughout the three Grand Regions (West, Middle, and East). The Regional Resource Liaisons shall be accountable to the State Resource Manager and TennCare for outreach, monitoring, engagement, Solution activity, and relationship management with the CBO partners. The Regional Resource Liaison shall be responsible for routine updates to the Community Resource Directory. The Regional Resource Liaisons shall be responsible for external and internal customer service management related to the Community Resource Directory in their respective region.	• A minimum of three (3) years of experience working with CBOs mission-focused on delivering basic needs/human service supports, including but not limited to housing, food, transportation, workforce, utility, or other related Domains. • A minimum of three (3) years of experience working with Tennessee CBOs with an approximate annual budget at or above \$1 million. • Strong understanding of safety net programs available in Tennessee. • Experience in managing recruitment, training, and retention efforts of MCOs, Providers, and CBOs for a IT solution similar in scale to the CLRS. • Experience in customer service management for a IT solution similar in scale to the CLRS.	• Shall be available for the entire term of the Contract and is expected to contribute at least 100% of annual Full-Time Equivalent (FTE) support to the specified role on the project. • Shall reside in the State of Tennessee. Any exceptions must be approved by TennCare. • Shall engage with existing participating CBOs (via in-person visits, virtual visits and/or phone/email communication) at least every six (6) months.
-----------------------------------	--	---	---

A.12.4. Facility

- A.12.4.1. TennCare may require certain Contractor personnel, as determined by TennCare, to work On-Site at TennCare offices located at 310 Great Circle Rd, Nashville, TN, or other permanent address of TennCare, at any point in the Contract.
- A.12.4.2. 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 at TennCare 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.12.4.3. The Contractor shall adhere to TennCare guidelines regarding health and safety while On-Site at the TennCare office.
- A.12.4.4. The Contractor shall leverage TennCare's video conferencing and collaboration licenses and tools (e.g., WebEx, Cisco TelePresence MX300 G2, Microsoft Teams, MX200 G2), where possible.
 - A.12.4.4.1. If the Contractor does not leverage TennCare's existing video conferencing and collaboration license of tools, the Contractor shall provide TennCare with access to a TennCare-approved Industry Standard teleconferencing service to allow for remote meetings at no additional cost to TennCare. Meetings, including On-Site meetings, shall be held remotely at the sole discretion of TennCare.
- A.12.4.5. The Contractor shall collaborate with TennCare to provide a facilities management plan for TennCare approval. The Contractor shall notify TennCare of any changes in the plan at least twenty (20) Business Days prior to the change.
- A.12.4.6. 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 the express written authorization from TennCare.
- A.12.4.7. The Contractor shall not allow Contractor's employees, agents, representatives, or sub-contractors to perform DDI or O&M activities on the Solution 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.12.4.8. 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 current IRS SCSEM, CMS MARS-E, SSA, and TennCare security framework.
- A.12.4.9. 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.12.5. Warranty

A.12.5.1. General Requirements

- A.12.5.1.1. The Contractor represents and warrants that the term of the warranty ("Warranty Period") for the Solution 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 goods 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.12.5.1.2. The Contractor represents and warrants that TennCare is authorized to possess and use all equipment, materials, software, and Deliverables provided under this Contract.
- A.12.5.1.3. 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.12.5.1.4. 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.12.5.1.5. The Contractor represents and warrants that each release of the Solution will conform to system requirements and expected outcomes as detailed in the functional design documentation, technical design documentation, and SSP as approved by TennCare.
- A.12.5.1.6. The Contractor represents and warrants that each subsequent Solution release will build upon and conform to previously released functionality, unless a change is explicitly approved by TennCare.
- A.12.5.1.7. If the Contractor is required under this Contract to perform Warranty work after Turnover of the Solution, the Contractor shall include Warranty Deliverables, testing, and any additional documentation requested by TennCare as part of the Turnover Plan.

A.12.5.2. Documentation and Resolution of Warranty Defects

- A.12.5.2.1. 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 and track Warranty Defects.
- A.12.5.2.2. The identification of critical and high Defects of the Solution during the Warranty Period shall extend the Warranty Period for the Solution for six (6) months after the time of the resolution of critical or high Defects.
- A.12.5.2.3. 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, 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.12.5.2.4. The Contractor shall resolve all medium and low Defects within the periods described in Contract Attachment B, Service Level Agreements and Liquidated Damages.

A.12.5.2.5. The Contractor shall be subject to corresponding Liquidated Damages, listed in Contract Attachment B, Service Level Agreements and Liquidated Damages, for all identified Warranty Defects that are not resolved within the associated resolution timeframes.

A.12.6. Change Order - Special Projects & Enhancements

A.12.6.1. 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.12.6.2. Changes Orders authorizing the scope of Services and funding for each Special Project or Enhancement shall be implemented by a Control Memorandum as described in A.12.7.

A.12.6.3. Support Change Requests

A.12.6.3.1. 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.12.6.3.2. The Contractor shall perform impact analysis on Change Requests to identify impacts across business processes and business rules.

A.12.6.3.3. The Contractor shall perform risk analysis on Change Requests to identify risks and potential mitigations associated with development and deployment of the change.

A.12.6.3.4. 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.12.6.3.5. The Contractor shall perform cost analysis for Change Requests as part of the Change Order process described in Section A.12.6. All Change Requests shall indicate implementation and full lifecycle costs for the proposed change.

A.12.6.3.6. 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.12.6.3.7. The Contractor shall provide analysis to support timing decisions for deployment of Change Requests in compliance with TennCare's release management process.

A.12.6.4. Change Order Creation

A.12.6.4.1. 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.12.6.4.1.1. 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 CLRS and any integrating CLRS, to include the written impact specifications of the corresponding CLRS Contractor;

- A.12.6.4.1.2. A description of the units of service needed to complete the change(s);
- A.12.6.4.1.3. The specific effort involved in completing the change(s);
- A.12.6.4.1.4. The expected schedule for completing the change(s);
- A.12.6.4.1.5. The maximum number of person hours required for the change(s); and
- A.12.6.4.1.6. 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.12.6.4.2. The Contractor shall not perform any Services under the Change Order until TennCare has approved the Change Order proposal through a 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.12.6.4.3. Subsequent to the 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.12.6.4.4. 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.12.7. Control Memorandum (CM) Process

- A.12.7.1. The 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 may 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. To the

extent possible, TennCare and Contractor will discuss all potential CMs prior to issuance by TennCare. However, nothing in this Contract shall be deemed to be a delegation to the Contractor of TennCare's non-delegable duties nor shall it be deemed to require Contractor's consent to, or agreement with, the subject matter of a CM prior to issuance by TennCare of a CM pertaining to any matter within the scope of this Contract.

- A.12.7.2. A CM may include one (1) or more of the five (5) components of the CM process described below:
 - A.12.7.2.1. On Request Report – a request directing the Contractor to provide information by the time and date set out in the CM;
 - A.12.7.2.2. 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.12.7.2.3. Notice of Potential Damages (Actual or Liquidated) (NPD) – notification to the Contractor that TennCare has determined that a potential Contract performance or compliance failure 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.12.7.2.4. 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 NCPDs may be issued consecutively or simultaneously; or
 - A.12.7.2.5. 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 NCPD. TennCare may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure. However, it is in TennCare's sole discretion to determine whether Actual Damages or Liquidated Damages will be assessed if a singular breach implicates both types of damages.
- A.12.7.3. 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.15., including Liquidated Damages as listed in Contract Attachment B, Service Level Agreements and Liquidated Damages, a Corrective Action Plan approved by TennCare, and/or termination of the Contract.
- A.12.7.4. Reconsideration of Damages Request by Contractor. Contractor may request reconsideration of 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 reconsideration request 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 reconsideration request determination or TennCare's Project Director (or his/her designee) is unable to resolve the reconsideration request, 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 reconsideration request 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 reconsideration request. TennCare's senior management shall provide written notice of its final determination to the Contractor within (10) Business Days of the receipt of the escalated reconsideration request from the Contractor. During the resolution of a reconsideration request or escalation, TennCare shall not increase the amount of the potential damages.

A.12.7.5. Implement Corrective Action Plan (CAP). 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) calendar 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.

A.12.7.5.1. 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. Each CAP shall, at a minimum, contain the following information:

- A.12.7.5.1.1. Written documentation that includes acknowledgment of receipt of TennCare notice;
- A.12.7.5.1.2. Number of impacted Members and cases and such other information as TennCare may request;
- A.12.7.5.1.3. A description of how the Contractor has addressed or will address the immediate Problem;
- A.12.7.5.1.4. An analysis of the root cause of the Problem; and
- A.12.7.5.1.5. A description of how the Contractor shall resolve the Problem (or has resolved the Problem) and shall prevent the Problem from recurring.

A.12.7.5.2. 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.12.7.5.3. The Contractor shall be responsible for ensuring that all of its subcontractors or service providers comply with all approved CAPs.

A.13. Training Requirements

A.13.1. General Training Requirements

- A.13.1.1. The Contractor shall collaborate with TennCare to identify, follow, and execute industry leading practices, standards, and trends for creation and delivery of training.
- A.13.1.2. The Contractor shall be capable of translating CLRS training materials to the five most common languages as outlined by <https://statisticalatlas.com/state/Tennessee/Languages> or determined by TennCare.
- A.13.1.3. The Contractor shall provide appropriate training and technical Subject Matter Professionals (SMPs) to lead the creation of training Artifacts and materials.
- A.13.1.4. The Contractor shall collaborate with TennCare to develop and provide a Training Plan that details all activities required to efficiently, accurately, and effectively train all identified end-users, Authorized Users, and technical staff that are expected to use or support maintenance of the Solution.
 - A.13.1.4.1.1. The Training Plan shall be developed in accordance with TennCare's overall training strategy and be approved by TennCare.
 - A.13.1.4.1.2. Once approved by TennCare, the Contractor shall be responsible for executing the Training Plan, as written, revised and approved, to comply with all TennCare-wide system and business operational standards, including service levels of the Solution.
 - A.13.1.4.1.3. The Contractor shall follow the TennCare Project Change Management Standard located in Attachment C, Procurement Library, including changes to the training scope, details, and approach, which will follow the project Change Management process.
 - A.13.1.4.1.4. The Contractor Training Plan shall include a comprehensive approach for TennCare including:
 - i) Maintain ongoing collaboration among TennCare and the Contractor;
 - ii) Detail training solution needs for highly technical staff responsible for maintaining the CLRS (technical staff), non-technical users (end-users), and the help desk, across all identified impacted Stakeholders;
 - iii) Identify learner groups within technical staff, end-users, and the help desk based on system roles, and map training curricula to each learner group;
 - iv) Identify role-based training curricula, including but not limited to training for technical staff, end-users, and the help desk with varying level of security access and administration privileges, that include business decisions and processes which integrate with Solution functionality;
 - v) Build, support, document, and maintain the accessible training environments necessary to support the delivery of technical staff, end-user, and help desk training;
 - vi) Provide necessary hardware and/or software installations to support both the development and delivery of training;
 - vii) Indicate the training facilities, equipment, and technology needed to support the proposed training plan;
 - viii) Define a timeline that encompasses all training-related activities and documents the dependencies between the training-related activities and other non-training activities (e.g., development, testing), including a go/no-go decision point criterion for training-related activities;

- ix) Outline the approach to the delivery of a Train-the-Trainer program and the delivery of technical staff and end-user training;
- x) Outline the approach to the delivery of the training to Authorized Users of CBOs;
- xi) Provide procedures for maintaining training documentation and conducting knowledge transfer sessions; and
- xii) Successfully create accessible training materials and job aids, including but not limited to user manuals, quick reference guides, Instructor-Led Training (ILT), Virtual Instructor-Led Training (VILT), eLearning, and all other documentation appropriate to the platform, operating systems, and programming languages.

A.13.1.5. The Contractor shall utilize a central training repository which will be identified by TennCare (i.e. SharePoint, Confluence, shared drives, etc.) for all training materials, which will provide an archive of 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 will be the property of TennCare and will be readily accessible and available On-demand to TennCare.

A.13.1.5.1. The Contractor shall build an “online help” functionality within the Solution. Online help is represented by online support for the Solution at a page level and for the system. Training materials, FAQs, and other support resources shall be available online and accessible from the banner menu or home page of the Solution. The online help shall include general and specific support on processes, screens, and functionality of the Solution. All identified technical staff, end-users, and help desk staff shall have access to the online help.

A.13.1.5.2. The Contractor shall provide support to all end-users, technical staff, and help desk staff in accessing and using the online help functionality while using any component of the Solution.

A.13.1.6. The Contractor shall deliver knowledge transfer sessions to identified technical staff, end-users, and help desk staff, including the management of the training environment(s) used for the development and delivery of training.

A.13.1.7. The Contractor shall collaborate with TennCare to leverage learner feedback to update training materials as needed and defined by TennCare.

A.13.2. Training Artifacts and Delivery

A.13.2.1. The Contractor shall submit training Artifacts including, but not limited to, templates, standards, outlines, and drafts for TennCare review and approval as defined and agreed upon in the Training Plan.

A.13.2.2. The Contractor shall be responsible for collaborating with TennCare to create training materials necessary to support the training of identified technical staff, end-users, and help desk staff.

A.13.2.2.1. The Contractor shall develop training materials that are role-based and include real-life scenarios for each learner group.

A.13.2.2.2. The Contractor shall develop training materials that include CLRS system functionality, business process, and policy information.

A.13.2.2.3. The Contractor shall provide training materials that include the following:

- i) Instructor-Led Training or Virtual Instructor-Led Training: Classroom based learning (either in a live or virtual setting) that includes “Tell Me, Show Me,

Let Me” opportunities for learners, including, but not limited to, PowerPoint presentations, guided practices, and independent practices. Instructor-led Training and/or virtual instructor-led training materials include, but are not limited to, PowerPoint presentations, facilitator guides, participant books, guided practices, independent Practices, data sheets, and any other material required to successfully deliver instructor-led training or virtual instructor-led training.

- ii) eLearning: On-demand learning assets that are available, accessible, and specific to technical staff, end-users, and/or help desk. eLearning material includes, but is not limited to, video tutorials, micro-learning, and web-based training courses.
- iii) Support Documentation: learning assets that are available to technical staff, end users, and help desk staff to aid in performing day-to-day tasks. Support documentation includes, but is not limited to, user guides, user manuals, quick reference guides, and standard operating procedures.

A.13.2.2.4. The Contractor shall be responsible for collaborating with TennCare and its partners to create knowledge transfer materials, including:

- A.13.2.2.4.1. Solution documentation for technical staff, and standard operating procedures and/or user, manuals for technical staff, end-users, and help desk staff;
- A.13.2.2.4.2. Train-the-Trainer session materials for individuals identified by TennCare to deliver additional end-user, technical staff, and help desk training sessions after the Contractor’s requirements have been fulfilled;
- A.13.2.2.4.3. Processes and procedures for updating all training materials;
- A.13.2.2.4.4. Processes and procedures for delivering all training activities;
- A.13.2.2.4.5. Processes and procedures for maintaining, updating, and leveraging the training environment and associated Data Sets for the development and delivery of training materials; and
- A.13.2.2.4.6. Materials shall be provided in advance of implementation to TennCare for review and approval.

A.13.2.2.5. The Contractor shall create, review, and update training materials in an agile, ongoing, iterative process as outlined by TennCare.

A.13.2.2.6. The Contractor shall validate system functionality prior to providing relevant training materials to TennCare for review and prior to delivering end-user, technical staff, and/or help desk training.

A.13.2.2.7. The Contractor shall identify and implement an appropriate review cycle format for all training Artifacts and materials, pending TennCare’s approval.

A.13.2.2.8. TennCare shall identify an overall approver for learning Artifacts and materials and identify reviewer(s) for each training Artifact and/or material, involving the appropriate SMP(s) based on their knowledge of the subject matter.

A.13.2.2.9. The Contractor shall ensure all materials are approved by TennCare prior to use and shall ensure all materials are reviewed and updated as continued Solution releases impact the effectiveness of the training materials as deemed necessary by TennCare.

A.13.2.2.10. The Contractor shall identify impacted Stakeholders, system training needs, and Solution training audience groupings.

- A.13.2.2.11. The Contractor shall develop detailed role-based curriculum maps, and pending approval, will create the identified training materials.
 - A.13.2.2.11.1. The Contractor shall collaborate with TennCare to determine the best training delivery method for each training audience grouping.
 - A.13.2.2.11.2. The Contractor shall provide general descriptions and other relevant course or material information.
- A.13.2.2.12. The Contractor shall provide Train-the-Trainer materials and deliver Train-the-Trainer to individuals identified by TennCare for end-user, technical staff, and help desk training.
- A.13.2.2.13. The Contractor shall conduct all technical staff, end-user, and help desk training.
 - A.13.2.2.13.1. The Contractor shall provide appropriate technical SMPs to attend trainings to provide active question and answer support, as well as training environment support.
 - A.13.2.2.13.2. The Contractor shall prepare and provide all soft copy and printed classroom training materials.
 - A.13.2.2.13.3. The Contractor shall develop the classroom training schedule, coordinate training facilities, facilitate training participant registration, and track and report on classroom training attendance and feedback.
- A.13.2.2.14. The Contractor shall identify any DDI update requiring a change in all training materials in a timely manner.
- A.13.2.2.15. After approval of a training material, the Contractor shall maintain training materials through 30 days after the completion of the Solution official Go-Live implementation. Training maintenance is defined as changes due to training material inaccuracies or system design clarifications. Other changes will go through the Change Request process. Training maintenance beyond 30 days after the completion of the implementation will be addressed by TennCare or through the CM process.
- A.13.2.2.16. The Contractor shall complete knowledge transfer of training development process, materials, and delivery with TennCare.
- A.13.2.2.17. The Contractor shall develop course feedback evaluations for TennCare to distribute to training participants following the delivery of all training events (e.g., vILT, ILT, eLearning).
 - A.13.2.2.17.1. The Contractor shall identify KPIs within the course evaluations.
 - A.13.2.2.17.2. The Contractor shall deploy course feedback evaluations following the conclusion of the training session (e.g., ILT, VILT, eLearning).
 - A.13.2.2.17.3. No later than two weeks following the course feedback evaluation completion, the Contractor shall complete an analysis and provide TennCare with a report-out and training artifact improvement recommendations.
- A.13.3. Training Technology and Tools
 - A.13.3.1. The Contractor shall establish a training environment strategy and approach, including, but not limited to, environment and data management.
 - A.13.3.2. The Contractor shall build and deliver training environments (build, stage/refresh data, and create training user accounts) to be ready in time for training activities.

- A.13.3.2.1. The Contractor shall collaborate with TennCare to identify the appropriate training data to be staged and included within the training environments.
- A.13.3.3. The Contractor shall perform training environment data refreshes and build upgrades during the training period which shall encompass the period through the end of the last day of end-user training as requested by TennCare.
- A.13.3.4. The Contractor shall test the Solution functionality in the training environment(s) after builds and on training days to confirm that the Solution is functioning as expected and will appropriately support training activities.
- A.13.3.5. The Contractor shall develop training environment user materials including, but not limited to, login instructions and accessing relevant components of the Solution.
- A.13.3.6. The Contractor shall manage access to the training environment through their Contract. No less than a month before the Contractor's Contract and service expiration, the Contractor shall complete knowledge transfer activities for the training environment with TennCare.

A.14. Table of Deliverables

- A.14.1. The Contractor shall refer to the CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables for the minimum requirements of the Contractor Deliverables during the Phased Implementation of the CLRS and Operational activities.
- A.14.2. The Contractor shall complete the Deliverables identified throughout the lifecycle phases of the TennCare Solution Implementation Lifecycle and CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables, as indicated in A.11. above. The TennCare Solution Implementation Lifecycle Standard 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 CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables Table of Deliverables is included below as Table 4: Table of Deliverables for reference purposes only.
- A.14.3. The Contractor shall ensure Deliverables also comply with the corresponding TennCare Standards Documentation, located in Attachment C, Procurement Library, where applicable.

TABLE 4: TABLE OF DELIVERABLES

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Concept Planning Requirements Review	Architecture Review Project Baseline Review Requirements Review	1. Project Management Plan	Baseline for project. High level PMP is initially approved during Concept phase and updated and approved once the Solution Vendor is on-boarded during Planning. It is updated as needed 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 Planning Requirements Review Development	Architecture Review Project Baseline 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 Planning. It is updated as needed 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 3. Validates planning and readiness of all parties, including trading partners, impacted by the interface(s).	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	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-	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			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 9. Conceptual Data Model and Dictionary 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.	Assessment and Roadmap to ensure that the project is advancing the capabilities of the business against the roadmap 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	
Planning	Project Baseline Review	4. Implementation Advanced Planning Document	APD/APD-U to describe the programmatic value, aligned to state priorities, that a state plans to achieve with their project. The APD/APD-U should include measurable outcomes and metrics that align with the desired Medicaid program goal(s). Contains: 1. Funding approval for the project 2. Requirements analysis 3. Feasibility study 4. Alternatives analysis 5. Cost allocation plan 6. Proposed budget	1. Validation by TennCare Accounting and Budget departments on the financial information 2. Validation from TennCare IS on the financial information 3. Validation from TennCare Strategic Funding and Compliance Officer 4. Approval from TennCare Deputy Commissioner	Type C
Planning	Project Baseline Review	5. Requirements Management Plan	Contains approach and methodology that the Solution Vendor will follow for managing requirements throughout the entire project.	Validation that: 1. The Requirements Management Plan is in alignment with TennCare Standards.	Type C
Requirements Review	Requirements Review	6. Requirements Traceability Matrix	The RTM contains the initial solution requirements and updated data requirements as published in the	Validation that: 1. The requirements in the RTM continue to align to TennCare's target state	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			RFP for a Solution Vendor. It is updated throughout the lifecycle of the project.	enterprise architecture and requirements as published in the RFP for a Solution Vendor. 2. The requirements meet the TennCare Data Policies and Standards. 3. Once the Solution Vendor is on-boarded, requirements are elaborated to a level of detail that is testable, with defined acceptance criteria. 4. The RTM approved at the Requirements Review Gate has the set of project level solution requirements traced to the complete set of original contract requirements, and traced to any CMS compliance criteria that are required for certification activities; with any exceptions annotated and approved. RTM: Traceability created, reports produced, updated continuously, reports generated as needed. *MORE:	
Requirements Review	Requirements Review	7. Conceptual Data Model and Dictionary	The Conceptual Data Model and Dictionary defines the information types or subject areas that are required to support the business capabilities that are in scope of a transformation effort as described in the Concept of Operations and the contract requirements. The Conceptual Data Model and Dictionary are initially created as part of the Concept of Operations document during the Concept Phase, and updated at the start of the Requirements Review Phase as part of reviewing data requirements.	Validation that: 1. The Conceptual Data Model and Dictionary meets the standards prescribed in the TennCare Data Policies and Standards 2. The TennCare Enterprise Architecture Modeling Standard 3. The TennCare Enterprise Architecture Framework	Type C
Requirements Review Design	Requirements Review Final Detailed Design Review	8. Logical Data Model and Dictionary	Define logical data models and dictionary that illustrate data concepts, entities, structures, and relationships to support the scope of the transformation effort. The logical data model does not prescribe physical data structures, but illustrates data requirements at a lower level of detail than the conceptual model. The logical model describes how data is related to itself, and business rules that must be enforced as a result of data requirements.	Acceptance Criteria	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Requirements Review	Requirements Review	9. 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	10. Integration Standard	The Integration Standard only applies to the ISL Vendor and was required for the ISL procurement. The Integration Standard outlines and describe the general integration strategy, approaches, and standards established for the project. These guidelines are to then be applied in developing the individual Interface Control Documents (ICDs) which define each individual interface that is to be implemented and/or managed as part of a module implementation.	Validation that: 1. The Solution Vendor has established integration standards for TennCare based on Enterprise Integration Patterns utilizing industry standard protocols and formats.	Type C
Requirements Review	Requirements Review	11. 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
Design	Final Detailed Design Review	12. 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	1. Validation that the deliverable includes acceptable plans and specifications, according to the Test Management Standard and the deliverable definition.	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			testing 14. Test reporting and metrics		
Design Implementation	Final Detailed Design Review Operational Readiness Review	13. Functional Design Document	Contains the detailed specifications that outlines the features and behavior of the solution. Will contain updated logical business and application architecture models (from the Concept of Operations Document) as per the TennCare Enterprise Architecture Modeling Standard, including but not limited to context models, business scenario models, 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. This document will cross-walk the data requirements against this updated application architecture. 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 and the data requirements are addressed by the detailed solution design.	Type C
Design Implementation	Final Detailed Design Review Operational Readiness Review	14. 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 6. Operational data design including how data should be created and maintained including Data Corrections, Data Retirement, Purge, Archive, and Retention - including defining secure disposal	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 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	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			and complete removal of data from all storage media 7. Design of how Metadata including Business Metadata, Data Quality Metadata, Technical Metadata, Operational Metadata, should be defined, documented, monitored, tracked and reported. Technical metadata should include Data Transformation and Data Lineage from system of record to identified field 8. Data ownership and accountability with assigned responsibilities defined, documented, and communicated as defined by the TennCare Data Policies and Standards 9. Design of how data will be transmitted and received by TennCare modules and repositories - specifying data flow information. 10. Design of data quality controls and monitors to meet the specified data quality requirements. 11. Design of data history capture and audit processes and data structures to meet requirements. 12. Completed data classification as defined by the TennCare Data Policies and Standards 13. All policies and procedures for Data acquisition and capture, Data backup and recovery, Data management and maintenance, and Data retention and secure destruction as defined by the TennCare Data Policies and Standards 14. All relevant External data Policies and Standards as defined by the TennCare Data Policies and Standards 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.		

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Design	Final Detailed Design Review	15. Interface Control Design Document	A comprehensive report of a system interface, including but not limited to, types of transactions and data requirements for Interfaces covered in External Interfaces Agreements (EIAs). 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. An Interface Control Design Document is required for every interface. The design of how the data will be converted from existing data sources to the new structure includes the data quality/transformation rules that will be applied. It will document how data will be transmitted and received by TennCare modules and repositories as defined by the TennCare Data Policies and Standards. Aligned with the TennCare Interface Landscape and Inventory. The Integration Plan outlines and describes the general integration strategy, approaches, and standards established for the project. These guidelines are to then be applied in developing the individual Interface Control Documents (ICDs) which define each individual interface that is to be implemented and/or managed as part of a module implementation. Use of a clear XML Schema Definition (XSD) to capture data type, cardinality, and conditionality for all elements within Web Services. Describes a Web Service (WS) connectivity strategy for lower environments should be established and documented. If real-time connectivity isn't available, consider using a mock service. Establishes alerts to trigger in the event of a loss	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

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			of connectivity with any inbound/outbound applications. Describes integration service contracts (e.g. API documentation) – including end points information.		
Design	Final Detailed Design Review	16. Data Sharing Agreement	The data sharing agreement is 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. The Solution Vendor shall provide a data sharing agreement for each Data Sharing Partner.	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	17. Infrastructure Plan	The detailed design of how the solution will be implemented either on premise 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
Design Implementation Operations & Maintenance	Final Detailed Design Review Operational Readiness Review Post-Implementation Review	18. Master Data Management Plan	The Master Data Management Plan includes 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. The MDM Plan	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
			will include the Master and Reference Data design and how it will be created, modified, deleted, accessed, and utilized as defined by the TennCare Data Policies and Standards.		
Design	Final Detailed Design Review	19. Data Management Plan	Will contain data conversion logical/technical architecture, including: 1. Mapping documents with associated business rules, strategy to profile, clean, and consolidate data. 2. The Data Transformation Mapping as defined in the EA Modeling Standard. 3. The design for data quality measures including Data Accuracy/Correctness, Completeness, Timeliness/Currency, Consistency/Uniqueness, Validity, Accessibility as defined by the TennCare Data Policies and Standards. 4. The approach, strategy, and architecture for using existing or creating new master and reference data as defined by the TennCare Data Policies and Standards.	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	20. Physical Database Design	A record layout of each data store with data element definitions. May contain the following artifacts defined in the EA Modeling Standard: Physical Data Model and 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	21. 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	Validation that: 1. The plan is developed in accordance with the TennCare Information Systems Lifecycle 2. The plan is developed in accordance with the Change Management Standard 3. Project Change Management Plan aligns with and is approved by TennCare's Enterprise Change Management Processes 4. Change Management Plan DED has	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			verifying that changes were made correctly	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	22. 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 9. Knowledge transfer programs for highly technical and non-technical Users across the Enterprise	Type C
Development	Validation Readiness Review	23. 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	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)	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			4. The mitigation plan for each outstanding defect	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	
Development	Validation Readiness Review	24. 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 workstreams 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
Development Implementation Operations & Maintenance	Validation Readiness Review Operational Readiness Review Post-Implementation Review	25. Physical Data Model and Dictionary	Define the physical data models and a dictionary that documents the implemented database structures. For SaaS products, a physical data model may be optional.	Validation that: 1. The deliverable aligns to the data requirements captured in the Technical Design Document, Requirements Traceability Matrix, and the Logical Data Model 2. The design is in alignment with TennCare modeling standards 3. The design is in alignment with TennCare Data Policies and Standards	Type C
Development	Validation Readiness Review	26. 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	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

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			5. Emergency contact information 6. Recovery Teams 7. Data and Solution Recovery 8. Communications Strategy 9. Identification and Backup of Essential Services 10. Recovery to pre-disaster state 11. Security and Alternative Security Strategy		
Development	Validation Readiness Review	27. 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 Contractor's general contact information for Incident notification and specific individual(s) with roles to contact in the event of a security or privacy Incident. 10. Describes how the Contractor 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	28. 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 Implementation and O&M. This is used at the very beginning of the project to ensure that proper	Validation that: 1. Information in the Security Management Plan Template meets or exceeds the required fields identified in the template.	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			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		
Test	Implementation Readiness Review	29. 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 Test (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	30. 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 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 5. The TennCare UAT testing team accepts the solution module	Type B
Test Operations & Maintenance	Implementation Readiness Review Post-Implementation Review	31. 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	Validation that: 1. The submitted schedule is in alignment with and addresses the requirements	Type D

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			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	defined in the deliverable expectations document and the deliverable definition.	

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			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. May contain the Security Boundary Model as defined in the EA Modeling Standard.		
Test Operations & Maintenance	Implementation Readiness Review Post-Implementation Review	32. 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 Privacy Impact Analysis (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	33. Information Security Risk Assessment	Utilizes CMS template report for Risks as a result of an identified Weakness [Plane of Action & Milestone (POAM)] 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	34. 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	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	Type B

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			passed, failed, and not completed 3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect	ORT or previous stages) have been resolved 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	35. 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	36. 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	37. Operations & Maintenance Run Book	Product documentation that describes how to operate the solution. Contains: 1. Operations manuals 2. Standard operating procedures (SOP) 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	Validation that: 1. The submitted deliverable is in alignment with and addresses the requirements defined in the deliverable expectations document and the deliverable definition.	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			8. Operations & Support procedures 9. System Configuration Document 10. Interface Descriptions/Controls including data flow between modules and repositories 11. System Operations Documentation 12. Training Artifacts 13. Training Plan 14. Updated Infrastructure System Source Code and Documentation 15. A substantive and representative set of all reports and information retrieval screens (electronic format preferred) 16. 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) 17. Plan for rolling out the new or updated module/system to the users 18. Implementation and Deployment Plan 19. Performance, Availability and Capacity Plan 20. Release and Deployment Plan 21. Service Transition Plan 22. System Maintenance, Support, and System Transition Plan 23. Cutover Plan 24. Description of how data should be created and maintained including Data Corrections, Data Retirement, Purge, Archive, and Retention, Data Quality controls and monitors, and data history capture and audit processes and data structures implemented to capture audit information (will also be captured in Physical Data Dictionary)		
Implementation	Operational Readiness Review	38. 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

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	39. 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 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 Post-Implementation Review	40. 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 POAM spreadsheet with the approval of the TennCare Chief Security Officer.	Validation that: 1. Risk and findings are logged in the CMS POAM format within the TennCare Governance Risk and Compliance (GRC) system. 2. Vendor completes monthly updates to all POAM's after initial submission 3. Vendor attends monthly POAM meetings with TennCare Security,	Type B
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	41. 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,	Validation that: 1. The full assessment report, associated report, and findings are provided to TennCare security and	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			operate as intended, and produce the desired outcomes for meeting the security and privacy 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) Certification. 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	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.	

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			6. Penetration Test and Scan Results Summary		
Implementation Operations & Maintenance	Operational Readiness Review Post-Implementation Review	42. Enterprise Intake Form	Intake Form will be customized for the state's ORR. For the ORR, the following steps are completed: The Intake Form Template is used throughout the Streamlined Modular Certification process to track information about a state MES project for certification. It is tailored for each state project. States will fill out the Intake Form Template by entering the CMS-required outcomes that document compliance with regulations applicable to their project, their state-specific outcomes, and the metrics used to show that the project is achieving its outcomes on a continuous basis. 1. The state completes the state columns of the Intake Form 2. The state saves related evidence and artifacts in a securely shared repository, accessible to CMS reviewers 3. At least two weeks before the ORR, the state sends the completed Intake Form to the CMS State Officer and to MES@cms.hhs.gov, giving CMS access to the evidence in the repository 4. Prior to the ORR, CMS will review the evidence, compile a list of any preliminary questions, and send those to the state to address during the ORR session. 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.	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	43. 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	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
				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	
Operations & Maintenance	Post-Implementation Review	44. Official Certification Request Letter	Required for 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 ISL meets all of the requirements of law and regulation: 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	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
			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	45. Metrics Report	Module-Specific metrics that demonstrate the system is meeting business objectives. Metrics that provide evidence that the outcomes are met on an ongoing basis. In accordance with 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), states must be capable of producing: 1. Data 2. Reports 3. Performance information from and about their MES modules All of which will be used to facilitate evaluation, continuous improvement in business operations, and transparency and accountability, as a condition for receiving enhanced federal matching for MES expenditures. The IS Solution Vendor will produce enterprise or IS-level data and reports for metrics reporting. Module-Specific and Enterprise Key Performance Indicators (KPI) are metrics 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. Metric reporting can be completed with appropriate results generated by the DDI vendor. 2. TennCare owners have signed off on each metric result to be reported	Type A
Retire	Disposition Review	45. 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	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	Type C

SILC Phase	Gate Review	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Review Cycle
			other systems impacted by the disposition	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 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 December 1, 2023 ("Effective Date") and extend for a period of THIRTY-SIX (36) 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 two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each 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 sixty (60) months.

C. PAYMENT TERMS AND CONDITIONS:

- C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed four million five hundred ninety-seven thousand eight hundred dollars and no cents (\$4,597,800.00) ("Maximum Liability"). The Maximum Liability shall include the Total Cost of DDI and O&M for the Term, Special Projects and Enhancements, and Authorized User subscription costs. 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.9.1.9. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - b) Data storage tools, capacity, and cost as required by A.9.1.10. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - c) Archiving tools, capacity, and cost as required by A.9.1.11. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - d) Data restore tools, capacity, and cost as required by A.9.1.12. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.
 - e) Cloud services as required by A.9.1.13. shall be included in the Maximum Liability and shall not result in additional cost to State of Tennessee or TennCare.
 - f) All costs associated with the facility as required by A.12.4. 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
 - g) All goods or Services, as applicable to the Solution, to satisfy the requirements in Sections A.3. through A.14. shall be included in the Maximum Liability and shall not result in additional cost to TennCare.

Notwithstanding the above, TennCare may, in its sole discretion, utilize alternative purchasing methods for purchases under this Contract, in whole or in part. In the event that TennCare utilizes alternative purchasing methods, in whole or in part, for any goods or services proposed by the Contractor, such costs as detailed in Attachment G, Schedule G shall be reduced from the Total Cost for DDI and O&M and Maximum Liability through an Amendment in accordance with D.3.

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 shall include all Deliverables and other activities required in the TennCare Solution Implementation Lifecycle. The standard method for Payment under this Contract to the 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 CLRS Solution.
 - 2) 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.
 - 3) 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 Phase Cost as described in this Section.
 - 4) 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 CM 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.
 - 5) 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.
 - 6) The alteration to the Payment and withhold structure shall be deemed to be made at the time that TennCare notifies the Contractor in writing.
 - 7) 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:

DDI Phase I	Gate Reviews	Gate Review Milestone Payment %	Gate Review Milestone Payments
Planning	Project Baseline Review	10%	\$ 72,750.00
Requirements Review	Requirements Review	20%	\$ 145,500.00
Design	Final Detailed Design Review	5%	\$ 36,375.00
Development	Validation Readiness Review	7%	\$ 50,925.00
Test	Implementation Readiness Review	8%	\$ 58,200.00
Issuance of State Acceptance Letter		20%	\$ 145,500.00
DDI Phase II	Gate Reviews	Gate Review Milestone Payment %	Gate Review Milestone Payments
Requirements Review	Requirements Review	4%	\$ 29,100.00
Design	Final Detailed Design Review	4%	\$ 29,100.00
Development	Validation Readiness Review	6%	\$ 43,650.00
Test	Implementation Readiness Review	6%	\$ 43,650.00
Additional Reviews		Additional Milestone Payment %	Additional Milestone Payments
Completion of Warranty		10%	\$ 72,750.00
Phased O&M		Annual Cost	
O&M Phase 1		\$ 582,000.00	
Solution O&M		Annual Cost	
Solution O&M		\$ 582,000.00	

The Contractor shall be compensated for Authorized User fees based upon the actual number of Authorized Users for the previous calendar month during the O&M Phase based on the payment methodology listed below.

All renewal options elected under this Contract will align with the Authorized Users Tier listed below.

Authorized Users	Monthly Cost
Unlimited (> 3001 Authorized Users)	\$ 97,000.00
Authorized Users Tier	Monthly Cost per Tier
Tier 1: 1-750 Authorized Users	\$ 77,600.00
Tier 2: 751-1500 Authorized Users	\$ 58,200.00
Tier 3: 1501-2550 Authorized Users	\$ 38,800.00
Tier 4: 2251-3000 Authorized Users	\$ 19,400.00

In the event that the State renews this Contract in accordance with B.2., the Contractor shall be compensated based on the following payment methodology.

O&M Optional Years	Annual Cost
Solution O&M Optional Year 1	\$ 582,000.00
Solution O&M Optional Year 2	\$ 582,000.00

- c) The Contractor shall be compensated for Special Project Change Orders and Enhancement Change Orders requested and performed pursuant to Contract Section A.12.6. 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, PROVIDED THAT:
- 1) Compensation to the Contractor for Special Project Change Orders shall not exceed ten percent (10%) 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 ten percent (10%) 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) 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	\$ 189,150 (10% of the Total DDI and O&M Costs)
Enhancement Change Order Request	\$ 189,150 (10% of the Total DDI and O&M Costs)

C.4. Performance Metric Payment. The Performance Metric Payment applies once the Contractor progresses to monthly payment for O&M Cost and Authorized User subscription cost, as specified in Section C.3. and Attachment G, Cost Proposal. The Performance Metric Payment shall represent up to fourteen percent (14%) of three (3) calendar months of monthly O&M Cost and Authorized User subscription cost, and shall be applied on a quarterly basis (three (3) calendar months).

- a) To guarantee Contractor's satisfactory and timely performance of the services and Deliverables set forth in this Contract, payment of up to fourteen percent (14%) of three (3) months of monthly O&M Cost and Authorized User subscription cost, for the Solution shall be based solely on Contractor's ability to satisfactorily perform and meet specific performance metrics selected for CBO engagement (Performance Metric Payment). The metrics will represent a high-priority subset of all the Contractor Services and Deliverables set forth in this Contract. Each performance metric will be weighted equally, unless otherwise specified by TennCare using the process described in Section C.4.b., to determine the percentage that each metric accounts for in the Performance Metric Payment.
- b) Following completion of DDI Phase 1, TennCare will use the CM Process described in Section A.12.7. to implement the performance metric used to determine the Performance Metric Payment based upon the Contractor's proposed performance metrics in Section C.4.e. Each Control Directive implementing the performance metrics may designate up to seven (7) Contract Services, Deliverables, or categories of Deliverables to be used as performance metrics. The Control Directive shall stipulate the performance parameters

and requirements for Contractor's performance to be considered acceptable and deemed as "PASS", and the level of performance below which TennCare deems performance to be unacceptable and deemed as "FAIL" for each performance metric.

- 1) The outcome of the Contractor's efforts on the performance metric will be measured each quarter (three (3) calendar months). Each performance metric shall be determined on a pass/fail basis by reference to the specific numerical performance requirement or completion of specific tasks as set forth in the Control Directive.
 - 2) The Control Directive shall also include any specific reporting requirements and the length of time the specified metrics will be used to determine the amount of the quarterly (three (3) calendar months) performance to be paid. At a minimum, any reporting or data needed to calculate the performance metric will be provided by the Contractor to TennCare within thirty (30) calendar days from the end of the performance metric quarter.
 - 3) The Contractor will continue to receive monthly O&M Cost and Authorized User subscription cost payments as invoiced to TennCare. Based on the results of the Contractor's performance on the performance metrics in effect for that quarter, TennCare will determine if any payment should be withheld for failure to meet any performance metric. If the Contractor has failed performance metric(s), TennCare will notify the Contractor in writing of the performance metric(s) failed and the corresponding Performance Metric Payment that is subject to be withheld from the next monthly O&M Cost and Authorized User subscription cost invoice payment.
 - 4) Upon written notification of the Contractor for failure to meet some or all of the performance requirements set forth in the Control Directive for a particular quarter, TennCare shall permanently withhold the applicable portion of the Performance Metric Payment from the next available O&M Cost and Authorized User subscription cost invoice to TennCare.
 - 5) Payment for the final O&M Cost and Authorized User subscription cost payment under the Contract Term shall be withheld until the final quarterly Performance Metric Payment is assessed, if applicable, by TennCare.
- c) Section C.4.e. to this Contract contains specific performance requirements that have been selected by TennCare to be the initial performance metrics.
- 1) TennCare may, in its sole discretion, and with a minimum of one quarter (three (3) calendar months) prior written notice, select any other Services or Deliverables required in the Contract to use as a performance metric for the purposes of determining the amount of the Performance Metric Payment to be paid by TennCare each month for achieving the performance metrics through the CM Process in A.12.7.
 - 2) In addition to selecting different performance metrics, TennCare may also use this one quarter (three (3) calendar months) written notice to change the weight of the selected performance metrics to be higher or lower through the CM Process in A.12.7.
 - 3) TennCare may use this one quarter (three (3) calendar months) written notice to adjust performance targets for specified metrics through the CM Process in A.12.7. Any adjustment to performance metrics will be informed by actual performance of the Contractor.
- d) TennCare, in its sole discretion, may elect to implement a performance metric measure on a test basis to verify the performance measure is providing TennCare with the intended outcomes before using that performance measure to determine Performance Metric Payment.

- 1) If TennCare elects to use a performance metric test, the applicable Control Directive will indicate a test period to be used for a specified performance measure, and the Contractor shall be required to adhere to the specifications in the Control Directive as if the performance measure being tested was formally being used to determine Performance Metric Payment. However, the pass/fail outcome of Contractor's compliance with the test performance measures shall not be used by TennCare to withhold any part of a monthly O&M Cost and Authorized User subscription cost invoice.
- e) Performance Metric Payment Calculation. As set forth in this Section C.4.e. using the initial performance metric Deliverables, illustrations and sample calculations used to determine Performance Metric Payments are shown below.

Performance Metric Category	Performance Metric	Score (PASS or FAIL)
Verified CBO Service Locations	The Contractor shall maintain a threshold of eighty percent (80%) of Verified CBO Service Locations by the end of DDI Phase I and one hundred percent (100%) of Verified CBO Service Locations by the end of DDI Phase II.	PASS/FAIL
Regional Threshold- Verified CBO Service Locations	The Contractor shall maintain of a threshold of 407 Verified CBO Service Locations in the East Grand Region by the end of DDI Phase I and 507 Verified CBO Service Locations in the East Grand Region by the end of DDI Phase II. The Contractor shall maintain of a threshold of 406 Verified CBO Service Locations in the Middle Grand Region by the end of DDI Phase I and 508 Verified CBO Service Locations in the Middle Grand Region by the end of DDI Phase II. The Contractor shall maintain of a threshold of 403 Verified CBO Service Locations in the West Grand Region by the end of DDI Phase I and 503 Verified CBO Service Locations in the West Grand Region by the end of DDI Phase II.	PASS/FAIL
Active CBO Service Locations	The Contractor shall maintain a specified threshold of twenty-five percent (25%) Active CBO Service Locations by the end of DDI Phase I. The Contractor shall maintain a specified threshold of thirty-three percent (33%) Active CBO Service Locations by the end of DDI Phase II.	PASS/FAIL
Regional Threshold-	The Contractor shall maintain a threshold of 132 Active CBO Service Locations in the East Grand Region by the	PASS/FAIL

Active CBO Service Locations	end of DDI Phase I and 169 Active CBO Service Locations in the East Grand Region by the end of DDI Phase II. The Contractor shall maintain a threshold of 133 Active CBO Service Locations in the Middle Grand Region by the end of DDI Phase I and 169 Active CBO Service Locations in the Middle Grand Region by the end of DDI Phase II. The Contractor shall maintain a threshold of 125 Active CBO Service Locations in the West Grand Region by the end of DDI Phase I and 166 Active CBO Service Locations in the West Grand Region by the end of DDI Phase II.	
Outreach	The Contractor shall contact new CBO Service Locations within ten (10) Business Days of adding the CBO Service Location to the Community Resource Directory. At least 95% of CBOs added to the Community Resource Directory must be contacted by the Contractor within the timeframe (10 Business Days) specified by TennCare.	PASS/FAIL
Solution Training	The Contractor shall complete training for eight-five percent (85%) CBO Service Locations within thirty (30) calendar days of being loaded into the Community Resource Directory.	PASS/FAIL
Closed-loops	The Contractor shall maintain a monthly average ratio of seventy-five percent (75%) Referrals to closed-loops that will be maintained throughout the quarter. The numerator in the calculation shall be the total monthly number of closed-loops and the denominator shall be the total monthly number of Referrals.	PASS/FAIL

- f) Performance Metric Payment Calculation. Per Contract Section C.4, up to fourteen percent (14%) of three (3) months of monthly O&M Cost and Authorized User subscription cost shall be contingent upon successful completion of the Contractor's performance metrics Pass/Fail score. The Contractor shall not be assessed more than fourteen percent (14%) of three (3) calendar months of monthly O&M Cost and Authorized User subscription cost on any one (1) monthly invoice. Each performance metric will be evaluated quarterly (three (3) calendar months) to determine if the Contractor passed or failed the performance metric. The Performance Metric Payment amount will be broken into quarterly (three (3) calendar months) installments to align with quarterly evaluation of the Contractor's performance on each performance metric. The number of performance metrics deemed "Failed" by TennCare will reduce the Performance Metric Payment as noted in the table below.

Number of Performance Metrics Failed	1	2	3	4	5	6	7
Amount of Performance Metric Payment deducted from monthly O&M Cost and Authorized User subscription cost payment	2%	4%	6%	8%	10%	12%	14%

C.5. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.6. 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:

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.
 - 5) 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 Section C.2 including, but not limited to:
 - a. Computing cost based on TennCare's cloud configuration by environment;
 - b. Network and telecommunication cost;
 - c. Data storage cost (active, infrequent, and archive) and data ingress-egress cost (in-transit); and
 - d. Transaction cost related to the number of reads, writes, and size of data packets.
 - 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.7. 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.8. 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.9. 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.10. 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 # 615-507-6443

The Contractor:

Chris Dunkin
Director of Government Markets
3429 Executive Center Drive
Austin, Tx 78731
cdunkin@findhelp.com
Telephone # 512-750-9490
FAX # 512-308-6846

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

- D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials. The State's exercise of a valid Renewal Option or Term Extension does not constitute an amendment so long as there are no other changes to the Contract's terms and conditions.
- 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 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, 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; 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 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, disqualified, or presently fall under any of the prohibitions of sections a-d.

- 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 State and federal laws and regulations applicable to Contractor in the Contractor's 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;
 - 3) Attachment C – Procurement Library;
 - i. CLRS TennCare Solution Implementation Lifecycle RACI and Deliverables
 - ii. TennCare Enterprise Architecture Framework Standard
 - iii. CLRS Volumetric Information
 - iv. TennCare Data Conversion Standard
 - v. TennCare Solution Implementation Lifecycle (SILC) Standard

- vi. TennCare Test Management Standard
- vii. TennCare Project Change Management Standard
- viii. TennCare Project Change Management Standard RACI
- ix. TennCare Project Management Plan Standard
- x. TennCare Preferred Technology Standard
- xi. TennCare Enterprise Architecture Modeling Standard
- xii. TennCare Requirements Management Standard
- xiii. TennCare IS Governance Standard
- xiv. TennCare Deliverable Template
- xv. TennCare IT Service Management Standard
- xvi. TennCare IT Service Management RACI
- xvii. TennCare Data Policies and Standards
- xviii. Industry Standards and Policies
- xix. TennCare Records Retention Policy
- xx. TennCare Records Disposition Authorization (RDA) List
- xxi. CMS Volume II: ACA Administering Entity System Security and Privacy Plan
- xxii. TennCare Privacy Program Policy and Plan (PRIV-028)
- xxiii. TennCare Privacy, Security and Confidentiality Training Policy (PRIV-013)
- xxiv. TennCare Organizational Chart
- xxv. Cloud Security Questionnaire
- xxvi. TennCare PCMH Practice Site EHRs Summary
- xxvii. CLRS Software License Supplemental Excel Template
- xxviii. TennCare Security Policies
 - a. TennCare Personnel Security Policy
 - b. TennCare Access Control Policy
 - c. TennCare Audit and Accountability Policy
 - d. TennCare Configuration Management Policy
 - e. TennCare Contingency Planning
 - f. TennCare Identification and Authentication Policy
 - g. TennCare Incident Response Policy
 - h. TennCare Maintenance Policy
 - i. TennCare Media Protection Policy
 - j. TennCare Physical and Environmental Protection Policy
 - k. TennCare Planning Policy
 - l. TennCare Program Management Policy

- m. TennCare Risk Assessment Policy
 - n. TennCare Security Assessment and Authorization Policy
 - o. TennCare Security Awareness and Training Policy
 - p. TennCare Security System and Information Integrity Policy
 - q. TennCare Security Systems and Communication Policy
 - r. TennCare System and Services Acquisition Policy
- 4) Attachment D – Requirements Traceability Overview and Matrix;
 - 5) Attachment E – Attestation Re: Personnel Use in Contract Performance;
 - 6) Attachment F – HIPAA Business Associate Agreement; and
 - 7) Attachment G – Cost Proposal.
- 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;
 - f) RFP # 31865-00635 Figure 1 – Closed-Loop Referral System Timeline; and
 - g) 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. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured on any insurance policy with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) insurance. All 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 shall provide the State evidence that all subcontractors maintain the required insurance or that subcontractors are included under the Contractor's policy. 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 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: (1)—all the insurance coverage and policy limits carried by the Contractor; or (2)—the minimum insurance coverage requirements and policy limits shown in this Contract; whichever is greater. Any insurance proceeds in excess of or broader than the minimum required coverage and minimum required policy limits, which are applicable to a given loss, shall be available to the State. 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) Technology Professional Liability (Errors & Omissions)/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 all acts, claims, errors, omissions, negligence, infringement of intellectual property (including copyright, patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, information theft, damage to destruction of or alteration of electronic information, breach of privacy perils, wrongful disclosure and release of private information, collection, or other negligence in the handling of Confidential Information, and including coverage for related regulatory fines, defenses, and penalties.
- 2) Such coverage shall include data breach response expenses, in an amount not less than ten million dollars (\$10,000,000) and payable whether incurred by the State or Contractor, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm

fees, credit file or identity monitoring or remediation services and expenses in the performance of services for the State or on behalf of the State hereunder.

e) Crime Insurance

- 1) The Contractor shall maintain crime insurance, which shall be written on a "loss sustained form" or "loss discovered form" providing coverage for third party fidelity, including cyber theft and extortion. The policy must allow for reporting of circumstances or incidents that may give rise to future claims, include an extended reporting period of no less than two (2) years with respect to events which occurred but were not reported during the term of the policy, and not contain a condition requiring an arrest or conviction.
- 2) Any crime insurance policy shall have a limit not less than one million dollars (\$1,000,000) per claim and one million dollars (\$1,000,000) in the aggregate. Any crime insurance policy shall contain a Social Engineering Fraud Endorsement with a limit of not less than two hundred and fifty thousand dollars (\$250,000). This insurance may be written on a claims-made basis, but in the event that coverage is cancelled or non-renewed, the Contractor shall purchase an extended reporting or "tail coverage" of at least two (2) years after the Term.

f) Professional Liability

- 1) Professional liability insurance shall be written on an occurrence basis or on a claims-made basis. If this coverage is written on a claims-made basis, then:
 - i. The retroactive date must be shown, and must be on or before the earlier of the Effective Date of the Contract or the beginning of Contract work or provision of goods and services;
 - ii. Insurance must be maintained and evidence of insurance must be provided for at least five (5) full years from the date of the final Contract payment; and
 - iii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or prior to the Contract Effective Date, the Contractor must purchase "extended reporting" or "tail coverage" for a minimum of five (5) full years from the date of the final Contract payment.
- 2) Any professional liability insurance policy shall have a limit not less than one million dollars (\$1,000,000) per claim and two million dollars (\$2,000,000) in the aggregate.

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.

The obligations set forth in this Section shall survive the termination of this Contract.

D.35. 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.

D.36. Boycott of Israel. The Contractor certifies that it is not currently engaged in, and covenants that it will not, for the duration of the Contract, engage in a Boycott of Israel, as that term is defined in Public Chapter No. 775.

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. 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 RFP # 31865-00635 (Attachment 6.2, Section B.15) 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.3. 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.4. 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.5. 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.
- E.6. 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.
- E.7. 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.8. 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.9. 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 Contractor intended to function with the Contract-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.
 - 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) 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.10. 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 found at the following URL: <https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html>.
- 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: The system shall preserve committed transactions in a manner that ensures no greater than 10 minutes of committed transaction data is lost as the result of an unplanned outage.
 - 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: Upon the declaration of a disaster, The Contractor will restore essential services, irrespective of the time the incident occurred, in less than or equal to four (4) hour 100% of the time.
- 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.11. 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.12. 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.13. 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.14. 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.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 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.12.7. 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 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, at no additional cost to the State, 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.12.7.
- 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 Contractor'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 (Implementation Date) specified by the State. The Implementation Date will typically coincide with the Successor Contractor's Go-Live Date pursuant to its contract with the State. However, the State may elect, in its sole discretion, to have the Contractor continue some portion of its services and systems after the Successor Contractor's Implementation Date, in which case, unless otherwise agreed to in writing by the State and Contractor, the Contractor shall be compensated for such services and systems in accordance with the provisions of Contract Section C. The Contractor shall be required to participate as directed by the State, at no additional cost, in assisting with the transition by providing specified deliverables, 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 an orderly transition of responsibilities. The Contractor shall, at all times, act in good faith toward the State and/or Successor Contractor to facilitate as seamless a transition as possible. The State will use the Control Memorandum process (as described in Section A.12.7.) 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. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. 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.

- 2) 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.

- b) The Contractor must report executive total compensation described above to the State by the end of the month during which this Contract is awarded.
- c) 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.
- d) 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 including, but not limited to D.34 (Confidentiality of Records), E.20 (Personally Identifiable Information), E.26 (Notification of Breach and Notification of Suspected Breach), E.28 Social Security Administration (SSA) Required Provisions for Data Security, and E.32 (Internal Revenue Service (IRS) Safeguarding Of Return Information) 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, 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.
- 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 maintain 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 the information is encrypted or if the transmittal is 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 notify 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.

- 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 Budget ("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
 - 2) Information 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.

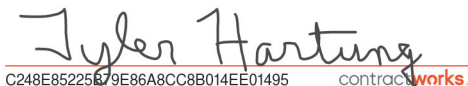
- E.33. Discovery and Litigation Hold Requirements. TennCare is frequently involved in litigation as either a party or a non-party with relevant information. Contractor shall cooperate with all TennCare requests to aid in data and document retention, and collection, as required for litigation. Contractor 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 contract, 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.
- g) Nondiscrimination Notice and Taglines. Should the Contractor create hardcopy and electronic materials related to the DDI of the Solution, the Contractor shall ensure that significant publications and significant communications, including small sized publications and communications that are targeted to beneficiaries, participants, end users, stakeholders, and members of the public shall contain the notice of nondiscrimination and LEP taglines as required by TennCare and set forth in TennCare's tagline templates and the applicable federal civil rights laws, including 45 C.F.R. pt 45. Materials shall be translated for individuals who are Limited English Proficient in accordance with the following requirements:
- (i) Pursuant to 68 Fed. Reg 47311-02, within ninety (90) calendar days of notification from TennCare, all vital Contractor documents related to this Contract shall be translated and available to each Limited English Proficiency ("LEP") group identified by TennCare in accordance with the applicable standards set forth below:
 - (ii) If a LEP group constitutes five percent (5%) or 1,000, whichever is less, of the population targeted under this Contract, vital documents shall be translated into that LEP language. Translation of other documents, if needed, can be provided orally; or
 - (iii) If there are fewer than fifty (50) individuals in a language group that is part the population targeted under this Contract that reaches the five percent (5%) trigger in (a), the Contractor shall inform those individuals that it does not provide written translation of vital documents but provides written notice in that group's primary language of the right to receive competent oral interpretation of those written materials, free of cost.
 - (iv) At a minimum, all vital Contractor documents shall be translated and available in Spanish and Arabic.

IN WITNESS WHEREOF,

AUNT BERTHA, A PUBLIC BENEFIT CORPORATION D.B.A. FINDHELP:


C248E85225679E86A8CC8B014EE01495 contractworks.

09/14/2023

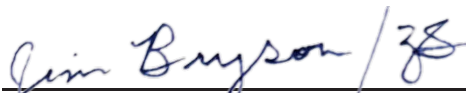
CONTRACTOR SIGNATURE

DATE

Tyler Hartung, VP of Finance

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF FINANCE AND ADMINISTRATION
DIVISION OF TENNCARE:


JIM BRYSON, COMMISSIONER

10/23/2023

DATE

CONTRACT ATTACHMENT A

DEFINITIONS AND ABBREVIATIONS

Located in the Procurement Library

CONTRACT ATTACHMENT B

SERVICE LEVEL AGREEMENTS AND LIQUIDATED DAMAGES

Located in the Procurement Library

CONTRACT ATTACHMENT C

PROCUREMENT LIBRARY

CONTRACT ATTACHMENT D

REQUIREMENTS TRACEABILITY OVERVIEW AND MATRIX

Located in the Procurement Library

CONTRACT ATTACHMENT E**ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE**

SUBJECT CONTRACT NUMBER:	CLRS 31865-00635
CONTRACTOR LEGAL ENTITY NAME:	Aunt Bertha, a Public Benefit Corporation
EDISON VENDOR IDENTIFICATION NUMBER:	0000250024

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.



C248E85225679E86A8CC8B014EE01495

contractworks.

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.

Tyler Hartung. VP of Finance**PRINTED NAME AND TITLE OF SIGNATORY**

09/14/2023

DATE OF ATTESTATION

CONTRACT ATTACHMENT F

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 Aunt Bertha, a Public Benefit Corporation, d/b/a findhelp® and findhelp.org® (“Business Associate”), located at 3429 Executive Center Drive, Austin, Texas 78731, 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:

CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF FINANCE AND ADMINISTRATION,
DIVISION OF TENNCARE
AND
AUNT BERTHA, A PUBLIC BENEFIT CORPORATION
D.B.A. FINDHELP

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:

Findhelp Information Security Manager: Richard Saunders
Findhelp Legal Notices: Dudley McClellan
3429 Executive Center Drive
Austin, Texas 78731
Email: security@findhelp.com
Email: legalnotices@findhelp.com

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 2.8 and 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 and 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 Section 6.3 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:
Dudley McClellan, Senior Counsel
Aunt Bertha, a Public Benefit Corporation
3429 Executive Center Drive
Austin, Texas 78731
Email: legalnotices@findhelp.com

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

By: Stephen Smith / 38
Stephen Smith, Director
 Date: 10/23/2023
 Division of TennCare

310 Great Circle Road
 Nashville, TN 37243
 Fax: (615) 253-5607

BUSINESS ASSOCIATE

By: Tyler Hartung
C248F85225679E86A8CC8B014EEF01495 contractworks
Tyler Hartung, VP of Finance
 Date: 09/14/2023

On behalf of:

Name: Aunt Bertha, a Public Benefit Corporation

Address: 3429 Executive Center Drive

Austin, Texas 78731

Email: thartung@findhelp.com

CONTRACT ATTACHMENT G

COST PROPOSAL