Teams, 2880 Gateway Oaks Drive, Suite 200, Sacramento, California, 95833. Notices mailed to the Contractor shall be to the address indicated on the coversheet of this Agreement.

5. Either party may change its address by written notice to the other party in accordance with this Section.

3.11 Information Confidentiality and Security

This Information Confidentiality and Security Requirements section sets forth the information privacy and security requirements the AAA is obligated to follow with respect to all personal, confidential, and sensitive information (as defined herein) disclosed to the AAA, or collected, created, maintained, stored, transmitted, or used by the AAA for or on behalf of the CDA pursuant to AAA's MOU with CDA and this Program Guide. (Such personal, confidential, and sensitive information is referred to here as CDA PSCI.) CDA and the AAA desire to protect their privacy and provide for the security of CDA PSCI pursuant to this section of the Program Guide and in compliance with state and federal laws applicable to CDA PSCI.

The terms of this section shall apply to all contracts, subcontracts, and subawards made by the AAA in furtherance of the MOU and services provided in accordance with this Program Guide. The AAA shall require its agents, subcontractors, or independent consultants (collectively, agents) to conform to this section regarding CDA PSCI.

3.11.1 Definitions

1. **Breach:**

   a. the unauthorized acquisition, access, use, or disclosure of CDA PSCI in a manner in which comprises the security, confidentiality, or integrity of the information; or

   b. the same definition of "breach of the security system" set forth in California Civil Code section 1798.29, subdivision (f); or

   c. the same as the definition of "breach" set forth in the Health Insurance Portability and Accountability Act Privacy Rule, 45 Code of Federal Regulations 164.402.

2. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code section 7920.000 Et seq.).

3. **Disclosure:** the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

4. **PSCI:** "personal information", "sensitive information", and "confidential information" (as these terms are defined herein).

5. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It is CDA's policy to consider all information about individuals private unless such information is determined to be a public record. Personal Information also includes the following:

a. Notice-Triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying information assigned to the individual, such as finger or voice print or a photograph. See Civil Code section 1798.29.

b. Protected Health Information (PHI): The term "PHI" refers to and includes both "PHI" as defined at 45 CFR section 160.103 and Personal Information (PI) as defined in the Information Practices Act at California Civil Code section 1798.3(a). PHI includes information in any form, including paper, oral, and electronic.

6. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 7920.000 Et seq.).

7. **Security Incident:**

a. A breach or attempted breach; or

b. The attempted or successful unauthorized access, disclosure, modification, or destruction of CDA PSCI, in violation of any state or federal law or in a manner not permitted under this Program Guide; or

c. the attempted or successful modification or destruction of, or interference with, the AAA's system operations in an information technology system, that negatively impacts the confidentiality, availability, or integrity of CDA PSCI; or

d. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

8. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher-than-normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

3.11.2 Disclosure Restrictions

The AAA shall protect CDA PSCI from unauthorized disclosure. The AAA shall not disclose, except as otherwise specifically permitted by the MOU and this Program Guide, any CDA PSCI to anyone other than CDA personnel or programs without prior written authorization from the CDA.

1. The AAA and CDA mutually agree that the creation, receipt, maintenance, transmittal, and disclosure of data from CDA containing PHI shall be subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing privacy and security regulations at 45 CFR Parts 160 and 164 (collectively and as used in this Agreement, HIPAA.). The AAA agrees to provide the same, or greater, level of protection to CDA data that would be required if the AAA were a Business Associate under HIPAA, regardless of whether the AAA is or is not a Business Associate.

2. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to CDA PSCI covered under this Program Guide beyond those provided through HIPAA, AAA agrees:

   a. To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

   b. To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate.

   c. Examples of laws that provide additional and/or stricter privacy protections to certain types of CDA PSCI, as defined in Section 3.11.1 of this Program Guide, include, but are not limited to the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

d. If the AAA is a Qualified Service Organization (QSO) as defined in 42 CFR section 2.11, the AAA agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) of that section.

3.11.3 Use Restrictions

The AAA shall not use any CDA PSCI for any purpose other than performing the AAA's obligations under the MOU and this Program Guide.

3.11.4 Safeguards and Security

The AAA shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of CDA PSCI including electronic CDA PSCI that it creates, receives, maintains, uses, or transmits on behalf of CDA. The AAA shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the AAA's operations and the nature and scope of its activities. The AAA's administrative, technical, and physical safeguards shall include, at a minimum:

1. Technical Security Controls:

The AAA shall, at a minimum, utilize a National Institute of Standards and Technology Special Publication (NIST SP) 800-53 compliant security framework when selecting and implementing its security controls and shall maintain continuous compliance with NIST SP 800-53 as it may be updated from time to time. The current version of NIST SP 800-53, Revision 5, is available online at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final; updates will be available online at https://csrc.nist.gov/publications/sp800.

2. Removable Media Devices

All electronic files that contain CDA PSCI data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, smart devices, tapes, etc.). PSCI must be encrypted, at a minimum, using a FIPS 140-2 certified algorithm or successor standards, such as Advanced Encryption Standard (AES), with a 128bit key or higher.

3. Patch Management:

The AAA shall apply security patches and upgrades and keep virus software up to date on all systems which PHI and other confidential information may be used.

4. Confidentiality Statement:

All people that will be working with CDA PSCI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by all people prior to accessing CDA PSCI. The statement must be

renewed annually. The AAA shall retain each person's written confidentiality statement for CDA inspection for a period of six (6) years following contract termination.

5. Transmission and Storage of PSCI:

All persons that will be working with CDA PSCI shall employ with FIPS 140-3 compliant encryption of PHI, at rest and in motion, unless it has been determined that such encryption is unreasonable and inappropriate based upon a risk assessment and equivalent alternative measures are in place and documented as such.

6. Minimum Necessary:

Only the minimum necessary amount of CDA PSCI required to perform necessary business functions applicable to the terms of this Program Guide may be used, disclosed, copied, downloaded, or exported.

7. Antivirus Software:

All workstations, laptops and other systems that process and/or store CDA PSCI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

8. Data Security:

CDA PSCI will be stored separately from other customers' data. Data will be stored and processed within the continental United States, and remote access to data from outside the continental United States will be prohibited. Data will be encrypted such that unauthorized parties are unable to read the data within the database/data repositories or any backups.

3.11.5 Employee Training

All persons who assist in the performance of functions or activities on behalf of CDA, or access or disclose CDA PSCI, must complete information privacy and security training, at least annually, at the AAA's expense. Each person who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

3.11.6 Employee Discipline

Appropriate sanctions must be applied against persons who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

3.11.7 Background Check

Before a person may access CDA PSCI, a thorough background check of that person must be conducted, with evaluation of the results to assure that there is no indication

that the person may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The AAA shall retain each person's background check documentation for a period of three (3) years following contract termination.

1. Mailing:

Mailings of CDA PSCI shall be sealed and secured from damage or inappropriate viewing of PSCI to the extent possible. Mailings which include 500 or more individually identifiable records of CDA PSCI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDA to use another method is obtained.

2. Security Officer:

The AAA shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with CDA.

3. Mitigation of Harmful Effects:

The AAA shall mitigate, to the extent practicable, any harmful effect that is known to the AAA of a use or disclosure of PSCI and other confidential information in violation of the requirements of this Program Guide.

4. Access to, and Accounting For, Disclosure of PSCI

The AAA shall document and make available to CDA or (at the direction of CDA) to an Individual such disclosures of CDA PSCI and information related to such disclosures necessary to respond to a proper request by the subject Individual for an accounting of disclosures of personal information as required by 45 CFR section 164.524 or any applicable state or federal law.

3.11.8 Access to Practices, Books, and Records

The AAA shall make its internal practices, books, and records relating to the use and disclosure of PSCI on behalf of CDA available to CDA upon reasonable request.

3.11.9 Special Provision for SSA Data

If the AAA receives data from or on behalf of CDA that was verified by or provided by the Social Security Administration (SSA Data) and is subject to an agreement between CDA and SSA, the AAA shall provide, upon request by CDA, a list of all employees and agents who have access to such data, including employees and agents of its agents, to CDA.

3.11.10 Breaches and Security Incidents

The AAA shall implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

1. Notice to CDA:

The AAA shall notify CDA immediately by email or telephone of the discovery of:

a. Unsecured CDA PSCI if the CDA PSCI is reasonably believed to have been accessed or acquired by an unauthorized person.

b. Any suspected security incident which risks unauthorized access to CDA PSCI and/or other confidential information.

c. Any intrusion or unauthorized access, use, or disclosure of CDA PSCI in violation of this Agreement; or

d. Potential loss of confidential data affecting this agreement.

e. Notice via email shall be made using the current CDA 1025 "Information Security Incident Report" forms and shall include all information known at the time the incident is reported. The forms are available online at: https://aging.ca.gov/Information_security/

f. Upon discovery of a breach or suspected security incident, intrusion, or unauthorized access, use or disclosure of CDA PSCI, the AAA shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and

ii. Any action pertaining to such unauthorized disclosure is required by applicable Federal and State laws and regulations.

2. Investigation of Security Incident or Breach

The AAA shall immediately investigate such security incident, breach, or unauthorized use or disclosure of CDA PSCI.

3. Complete Report

The AAA shall provide a complete report of the investigation to CDA within (10) working days of the discovery of the breach or unauthorized use or disclosure. The complete report must include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable federal and state laws. The report shall include a full, detailed corrective action plan including information on measures that were taken to halt and/or contain improper use or disclosure. If CDA requests information in addition to this report, the AAA shall make reasonable efforts to provide CDA with such information. CDA will review and approve or disapprove the AAA's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and the AAA's corrective action plan.

a. If the AAA does not submit a complete report within the ten (10) working day timeframe, the AAA shall request approval from CDA within the ten (10) working day timeframe of a new submission timeframe for the complete report.

4. Notification of Individuals

If the cause of a breach is attributable to the AAA or its agents, the AAA shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply with applicable federal and state law. CDA shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made.

5. Responsibility for Reporting Breaches to Entities other than CDA

If the cause of a breach of CDA PSCI is attributable to the AAA or its subcontractors, the AAA is responsible for all required reporting of the breach as required by applicable federal and state law.

6. Submission of Sample Notification to Attorney General:

If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, regardless of whether the AAA is considered only a custodian and/or non-owner of the CDA PSCI, the AAA shall, at its sole expense and at the sole election of CDA, either:

a. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). The AAA shall inform the CDA Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or

b. Cooperate with and assist CDA in its submission of a sample copy of the notification to the Attorney General.

3.11.11 Contact Information

To direct communications to the above referenced CDA staff, the AAA shall initiate contact as indicated herein. CDA reserves the right to make changes to the contact information below by giving written notice to the AAA.

CDA Privacy Officer	CDA Information Security Officer
Office of Legal Services 2880 Gateway Oaks Dr. Suite 200 Sacramento, CA 95833 Attn: Chief Counsel Email: privacy@aging.ca.gov Telephone: (916) 419-7500	Information Security Branch 2880 Gateway Oaks Dr. Suite 200 Sacramento, CA 95833 Attn: Information Security Officer Email: iso@aging.ca.gov Telephone: (916) 419-7500

3.11.12 Responsibility of CDA

CDA agrees to not request the AAA use or disclose PSCI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

3.11.13 Audits, Inspections, and Enforcement

1. CDA Right to Inspect:

From time to time, CDA may inspect the facilities, systems, books, and records of the AAA to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) section. The AAA shall promptly remedy any violation of any provision of this ICSR section. The fact that CDA inspects, or fails to inspect, or has the right to inspect, the AAA's facilities, systems, and procedures does not relieve the AAA of its responsibility to comply with this ICSR section.

2. Notification to CDA in Event the AAA is Subject to Other Audit:

If the AAA is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to the MOU and/or this Program Guide or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, the AAA shall promptly notify CDA unless it is legally prohibited from doing so.

3.11.14 Miscellaneous Provisions

1. Disclaimer:

CDA makes no warranty or representation that compliance by the AAA with this Program Guide will satisfy the AAA's business needs or compliance obligations. The AAA is solely responsible for all decisions made by the AAA regarding the safeguarding of CDA PSCI and other confidential information.

2. Amendment:

a. Any provision of the MOU or this Program Guide which conflicts with current or future applicable federal or state laws is hereby amended to conform to the provisions of those laws. Such amendment of the MOU and/or this Program Guide shall be effective on the effective date of the laws necessitating it and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

b. Failure by the AAA to take necessary actions required by amendments to the MOU and/or this Program Guide shall constitute a material violation.

3. Assistance in Litigation or Administrative Proceedings

The AAA shall make itself, its employees, and agents available to CDA at no cost to CDA to testify as witnesses in the event of litigation or administrative proceedings being commenced against CDA, its director, officers, or employees based upon claimed violation of laws relating to security and privacy, and which involves inactions or actions by the AAA (except where the AAA or its subcontractor, workforce employee, or agent is a named adverse party).

4. No Third-Party Beneficiaries

Nothing in this Program Guide is intended to or shall confer upon any third person, any rights, or remedies whatsoever.

5. Interpretation

The terms and conditions in this Program Guide shall be interpreted as broadly as necessary to implement and comply with regulations and applicable laws. The parties agree that any ambiguity in the terms and conditions of this Program Guide shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

6. No Waiver of Obligations

No change, waiver, or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation or shall prohibit enforcement of any obligation on any other occasion.

7. Return or Destruction of CDA PSCI on Expiration or Termination

At expiration or termination of the MOU, if feasible, the AAA shall return or destroy all CDA PSCI that the AAA still maintains in any form and retain no copies of such information. If return or destruction is not feasible, CDA and the AAA shall determine the terms and conditions under which the AAA may retain the PSCI.

8. Data Sanitization

All CDA PSCI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDA PSCI is no longer needed.

a. Survival

If return or destruction of CDA PSCI is not feasible upon the completion or termination of the MOU, the respective rights, and obligations of the AAA under this Section shall survive the completion or termination of the MOU between the AAA and CDA. The AAA shall also limit further uses and disclosures of CDA PSCI to those purposes that make the return or destruction of the information infeasible.

3.12 Copyrights and Rights in Data

3.12.1 Copyrights

1. If any material funded by CDA is subject to copyright, the State reserves the right to copyright such material and the AAA agrees not to copyright such material, except as set forth in Section 3.12.2.

2. The AAA may request permission to copyright material by writing to the Director of CDA. The Director shall grant permission or give reason for denying permission to the AAA in writing within sixty (60) days of receipt of the request.

3. If the material is copyrighted with the consent of CDA, the State reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, prepare derivative works, publish, distribute and use such materials, in whole or in part, and to authorize others to do so, provided written credit is given to the author.

4. The AAA certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of work outlined within this Program Guide or the MOU for the acquisition, operation, or maintenance of computer software in violation of copyright laws.

3.12.2 Rights in Data

1. The AAA shall not publish or transfer any materials, as defined in item 2 below, produced or resulting from activities supported by this Program Guide and the MOU without the express written consent of the Director of CDA. That consent shall be given, or the reasons for denial shall be given, and any conditions under which it is given or denied, within thirty (30) days after the written request is received by CDA. CDA may request a copy of the material for review prior to approval of the request. This subsection is not intended to prohibit the AAA from sharing identifying client information authorized by the participant or summary program information which is not client-specific.

2. As used in this Program Guide, the term “subject data” means writings, sound recordings, pictorial reproductions, drawings, designs or graphic