

## DEPARTMENT OF HEALTH CARE SERVICES

### AGREEMENT FOR DISCLOSURE AND USE OF MEDI-CAL DATA

In order to secure data and documents that reside in the California Department of Health Care Services (DHCS) Medi-Cal systems of records, or with its agents, and to ensure the integrity, security, and confidentiality of such data and documents, and to permit only appropriate disclosure and use as may be permitted by law, DHCS and Trinity Technology Group (User) enter into this Agreement to comply with the following specific sections. This Agreement shall be binding on any successors to the parties.

1. This Agreement is by and between the California Department of Health Care Services and the Trinity Technology Group.
2. This Agreement addresses the conditions under which DHCS will disclose and the User(s) will obtain and use Medi-Cal data file(s) as set out in Attachment A. This Agreement supplements any agreements between the parties with respect to the use of information from data and documents and overrides any contrary instructions, directions, agreements, or other understandings in or pertaining to any other prior communication from DHCS or any of its components with respect to the data specified in this Agreement. The terms of this Agreement may be changed only by a written modification to this Agreement or by the parties entering into a new agreement. The parties agree further that instructions or interpretations issued to the User(s) concerning this Agreement, and the data and documents specified herein, shall not be valid unless issued in writing by the DHCS point-of-contact specified in Section 4 or the DHCS signatories to this Agreement shown in Section 22.
3. The parties mutually agree that the following named individuals are designated as "Custodians of the Files" on behalf of the User(s) and shall be responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use or disclosure. The User(s) agree to notify DHCS within fifteen (15) days of any change to the custodianship information.

**Christopher Worley**

\_\_\_\_\_  
(Name of Custodian of Files)

**Project Manager**

\_\_\_\_\_  
(Title/Component)

**Trinity Technology Group**

\_\_\_\_\_  
(Company/Organization)

**2015 J Street, Suite 105, Sacramento, CA 95811**

\_\_\_\_\_  
(Company Address)

Page 1 of 8

User Initial:   *CMW*  

DUA #RFO-AI2014-02

4. The parties mutually agree that the following named individual will be designated as “point-of-contact” for the Agreement on behalf of DHCS.

**Bob Sands**

(Name of Contact)

**Assistant Deputy Director, Audits and Investigations**

(Title/Component)

**916-650-6685; bob.sands@dhcs.ca.gov**

(Phone Number / Email Address)

5. The parties mutually agree that the following specified Attachments are part of this Agreement:

Attachment A: Data Files

Attachment B: SSA Agreement

Attachment C: Security Controls

Attachment D: Notification of Breach

6. The parties mutually agree, and in furnishing data files hereunder DHCS relies upon such agreement, that such data file(s) will be used solely for the following purpose:

DHCS is the single source of Medicaid (Medi-Cal) administration for the State of California. DHCS’ duties include avoiding and detecting fraud, waste and abuse in the Medi-Cal system. One of the ways DHCS accomplishes these duties is through the use of data analytics, performed on its systems, including MIS-DSS and the Short-Doyle/Medi-Cal (SDMC) system. The SDMC is the State’s automated adjudication system for behavioral health claims. The SDMC system applies accepted business rules to behavioral health care claims and drug Medi-Cal claims submitted by California counties, business associates and a large number of direct providers. These rules, along with State reimbursement rate tables, provide detail needed to adjudicate the claims.

The services to be provided in connection with RFO# AI-2014-02 are a continuation of the work done under RFO# AI-2013-01, including detecting and linking fraud schemes and identifying high-risk providers using data mining and various information databases/tools to identify fraud and outlier behavior in the Medi-Cal program. Under RFO#AI-2014-02, DHCS will include additional data sources to improve capacity for detecting and linking fraud schemes.

Services will include identifying potential instances of fraud and/or abuse, which will be analyzed by DHCS investigators, auditors, analysts and legal staff. The potential instances identified must be provided in User’s reports to DHCS, which will include but not be limited to the following: findings, leads, fraud indicators, and aberrant billing patterns. The User(s) must be able to provide cogent explanations to the DHCS team as to why individual alerts were identified by the data analytics tool. The User(s) must produce various sets of reports as requested by

User Initial: CMW

DHCS, as well as securely transferring files containing suspicious cases, and/or providing DHCS access to the data solution, including a dashboard.

The parties understand and agree that, due to the nature of the data stored on the SDMC system and the MIS/DSS data warehouse, as well as the data linkage and detection required in order to perform the fraud and abuse investigations required under the parties' Agreement, these data constitute the minimum necessary for the purpose of the project, as contemplated by HIPAA. The parties further agree that the purposes of this Agreement are directly connected to the administration of the Medi-Cal program, and that no personally identifiable data will be disclosed to anyone, and no individual identified, other than as provided in this Agreement.

7. Some of the data specified in this Agreement may constitute Protected Health Information (PHI), including protected health information in electronic media (ePHI), under federal law, and personal information (PI) under state law. The parties mutually agree that the creation, receipt, maintenance, transmittal and disclosure of data from DHCS containing PHI or PI shall be subject to the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act) and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 (HIPAA regulations), the Final Omnibus Rule, the provisions of the California Information Practices Act, Civil Code section 1798 *et. seq.*, 42 CFR Part 2, and the provisions of other applicable federal and state law. User(s) specifically agree they will not use the Attachment A data for any purpose other than that stated in paragraph 6 of this Agreement. User(s) also specifically agree they will not use any DHCS data, by itself or in combination with any other data from any source, whether publicly available or not, to individually identify any person to anyone other than DHCS as provided in this Agreement.
8. The following definitions shall apply to this Agreement. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations or other applicable law. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.
  - a. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, the Final Omnibus Rule, and the California Information Practices Act.
  - b. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

User Initial: CMW

- c. Personal Information (PI) shall have the meaning given to such term in Civil Code section 1798.29.
  - d. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
  - e. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
  - f. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the User's organization and intended for internal use; or interference with system operations in an information system.
  - g. Unsecured PHI shall have the meaning given to such term under the HITECH Act, any guidance issued pursuant to such Act including, but not limited to, 42 USC section 17932(h), the HIPAA regulations and the Final Omnibus Rule.
9. The User(s) represent and warrant that, except as DHCS shall authorize in writing, the User(s) shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person, company or organization. The User(s) agrees that, within the User(s)' organizations, access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this Agreement or Attachment A and to those individuals on a need-to-know basis only. User(s) shall not use or further disclose the information other than is permitted by this Agreement or as otherwise required by law. The User(s) shall not use the information to identify or contact any individuals.

User Initial:   CMW  

DUA #RFO-AI2014-02

10. The User(s) agree to notify DHCS within 30 days of the completion of the purpose specified in section 6. Upon such completion, the User(s) shall destroy all electronic data files with DHCS data by wiping such data using Department of Defense standards or as approved by DHCS. The User(s) shall destroy all paper documents with DHCS data by using a confidential method of destruction, such as crosscut shredding or contracting with a company that specializes in confidential destruction of documents. The User(s) shall certify the destruction of the file(s) in writing within 30 days of the destruction. A statement certifying this action must be sent to the DHCS point-of-contact listed in section 4. The User(s) agree that no data from DHCS records, any parts or copies thereof, including files derived from DHCS records (electronic, hardcopy or otherwise), shall be retained when the files are destroyed unless authorization in writing for the retention of such files has been received from the DHCS person designated in section 4.
11. The User(s) agree to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established in HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Final Omnibus Rule as set forth in 45 CFR, parts 160, 162 and 164 of the HIPAA Privacy and Security Regulations. The User(s) also agree to provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies. If the data obtained by User(s) from DHCS includes data provided to DHCS by the Social Security Administration (SSA), User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment B and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. In addition, the User(s) agree to comply with the specific security controls enumerated in Attachment C of this Agreement. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide DHCS data, agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.
12. The User(s) acknowledge that in addition to the requirements of this Agreement, they must also abide by the privacy and disclosure laws and regulations under 45 CFR Parts 160 and 164, of the HIPAA regulations, section 14100.2 of the California Welfare & Institutions Code, Civil Code section 1798.3 et. seq. and the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, as well as any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.

User Initial: CMW

DUA #RFO-AI2014-02

The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide the DHCS data, agree to the same restrictions and conditions that apply to the User(s) with respect to such information.

13. The User(s) agree to report to DHCS any use or disclosure of the information not provided for by this Agreement of which it becomes aware, immediately upon discovery, and to take further action regarding the use or disclosure as specified in Attachment D, Notification of Breach, of this Agreement.
14. User(s) agree to train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data, and to discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment. In complying with the provisions of this section, User(s) shall observe the following requirements:
  - (a) User(s) shall provide information privacy and security training, at least annually, at its own expense, to all its employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data; and
  - (b) User(s) shall require each employee who receives information privacy and security training to sign a certification, indicating the employee's name and the date on which the training was completed.
15. From time to time, DHCS may, upon prior written notice and at mutually convenient times, inspect the facilities, systems, books and records of User(s) to monitor compliance with this Agreement. User(s) shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, User(s)' facilities, systems and procedures does not relieve User(s) of their responsibility to comply with this Agreement.
16. The User(s) acknowledge that penalties under 45 CFR, parts 160, 162 and 164 of the HIPAA regulations, and section 14100.2 of the California Welfare & Institutions Code, including possible fines and imprisonment, may apply with respect to any disclosure of information in the file(s) that is inconsistent with the terms of this Agreement. The User(s) further acknowledge that criminal penalties under the Confidentiality of Medical Information Act (Civ. Code § 56) may apply if it is determined that the User(s), or any individual employed or affiliated therewith, knowingly and willfully obtained any data under false pretenses.
17. By signing this Agreement, the User(s) agree to abide by all provisions set out in this Agreement and in Attachments B, C and D and for protection of the data file(s) specified in this Agreement, and acknowledge having received notice of potential criminal, administrative, or civil penalties for violation of the terms of the Agreement. Further, the User(s) agree that any material violations of the terms of this Agreement or any of the laws and regulations governing the use of DHCS data may result in denial of access to DHCS data.

User Initial:   CMW



18. This Agreement shall terminate at the time of the completion of the project which is described in paragraph 6, or one year after the date it is executed, whichever event occurs later, and at that time all data provided by DHCS must be destroyed as set forth in Section 10, above, and a certificate of destruction sent to the DHCS representative named in Section 4, unless data has been destroyed prior to the termination date and a certificate of destruction sent to DHCS. All representations, warranties and certifications shall survive termination.

Termination for Cause. Upon DHCS' knowledge of a material breach or violation of this Agreement by User(s), DHCS may provide an opportunity for User(s) to cure the breach or end the violation and may terminate this Agreement if User(s) does not cure the breach or end the violation within the time specified by DHCS. DHCS may terminate this Agreement immediately if User(s) breach a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, User must destroy all PHI and PI in accordance with Section 10, above. The provisions of this Agreement governing the privacy and security of the PHI and PCI shall remain in effect until all PHI and PI is destroyed or returned to DHCS.

19. This Agreement may be signed in counterpart and all parts taken together shall constitute one agreement.
20. The Custodian, as named in Section 3, hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User(s), and agrees in a representative capacity to comply with all of the provisions of this Agreement on behalf of the User(s).

Christopher Worley \_\_\_\_\_  
(Name of Custodian of File(s) - Typed or Printed)

Project Manager \_\_\_\_\_  
(Title/Component)

 \_\_\_\_\_  
(Signature)

June 5, 2015 \_\_\_\_\_  
(Date)

21. On behalf of the User(s), the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Stephen Williamson \_\_\_\_\_  
(Name - Typed or Printed)

Partner \_\_\_\_\_  
(Title/Component)


Trinity Technology Group \_\_\_\_\_  
(Company/Organization)

User Initial: CMW \_\_\_\_\_

2015 J Street, Suite 105  
(Address)

Sacramento, CA 95811  
(City/State/ZIP Code)

916-779-0220; svwilliamson@trinitytg.com  
(Phone Number and E-Mail Address)

  
(Signature)

June 8, 2015  
(Date)


22. On behalf of DHCS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Bob Sands  
(Name of DHCS Representative - Typed or Printed)

Assistant Deputy Director, Audits and Investigations  
(Title/Component)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

User Initial: 



The vendor will not have direct access to any DHCS systems or files, but instead a DHCS employee will create data extracts files which will be sent securely to the vendor for analysis at their facility. Files sent to or from DHCS will be encrypted with Zip 256bit AES, and transferred with SSL encryption. Other methods of transfer will require approval by the DHCS Information Security Officer. Each individual request for data will require DHCS review and approval of the specific data elements, and a justification must be provided.

The contents of the data extract files will be governed by the Data Release forms, which will get down to the data element level for fields which contain PHI/PI.

The primary source of data for the data extracts as input to the data analytics services to identify potential sources of fraud and abuse in the behavioral health programs will be the Short-Doyle Medi-Cal (SMDC) database.

Since SDMC does not contain all of the data which would be useful in identifying potential fraud and abuse in the behavioral health programs, the vendors will also obtain extract information from the following secondary sources of information:

- **Strike Team provider database**  
This is Excel spreadsheet developed by A&I Strike Team. The file includes the facility name, first and last names of any personnel that are found on their financial/management documents, AKAs, Board of Directors, and positions with the company; if known.
- **USL database**  
This system contains additional claim information, which is not contained on the SDMC database
- **Mental Health provider database**  
This file includes address information for providers, which can be used for geo-spatial data analytics
- **SMART database**  
The SMART database contains claim information for substance abuse services.
- **MEDS database**  
This is the system which captures information about eligibility for Medi-Cal and other health-related government programs. Access to data system to be as determined necessary by DHCS and vendor; no direct access to DHCS' systems shall be allowed. Vendor shall at all times be under direct supervision by the appropriate (as determined by DHCS) employee when DHCS data is being viewed, disclosed or used by vendor. ITSD staff will provide data matches of the beneficiary phone numbers and e-mail addresses for the sole

purpose of identifying potential anomalies such as persons not in the same household sharing a phone number, which might indicate potential fraud, but under no circumstances may A&I or the vendor utilize this information to contact any beneficiaries.

- MIS/DSS database  
This is the Department's data warehouse which includes diagnosis, claim, eligibility and provider information. Access to data system to be as determined necessary by DHCS and vendor; no direct access to DHCS' systems shall be allowed.
- PAVE  
This database contains enrollment, verification and report data about current and prospective Medi-Cal providers.
- Public Requests Act (PRA) database  
This database contains a list of all PRA requests received in 2014 and in subsequent years. The purpose for accessing this database is that investigative reporters may have leads about potential fraud and abuse in the Medi-Cal program.
- CalOMS - a statewide treatment and prevention outcomes measurement system that provides information for administering and improving prevention and treatment programs
- Provider Master File - Medi-Cal provider data including provider type, license numbers, provider name, address, birthdate, and gender
- Capitated Payment Management System (CapMan) - managed care beneficiary and payment data
- Paid Claim Encounter System (PCES) - encounter data on managed care beneficiaries
- Cal MediConnect - encounter data on dual eligible managed care beneficiaries
- LexisNexis
- TransUnion (TLO)
- Dun & Bradstreet
- Appriss (JusticeXchange tool)

- Social Intelligence Corp (Riv Data)

## Pondera and CA DHCS Data Use Agreement – Appendix E

### Continuous Auditing and Monitoring Program Requirements

#### PURPOSE

Pondera Solutions Information Security Program provides the highest level of policy to ensure Pondera Solutions information systems adhere to and are in compliance with all established laws and regulations. This DUA Appendix document describes the level of process, procedures, and responsibilities relative to Pondera’s Information Security Continuous Monitoring (ISCM) program.

The intent of this document is to inform CA DHCS on Pondera ISCM requirements, specifically:

- (1) The requirements of the initial End-User audit process(es);
- (2) The requirements of the periodic on-going End-User audit process(es);
- (3) The requirements of the randomized End-User audit process(es);
- (4) Which individuals are responsible for specific tasks; and
- (5) How other information security activities relate to and/or interact with the ISCM auditing processes.

#### SCOPE

##### Applicability:

- (1) The policies stated in this DUA Appendix document apply to all individuals (Pondera employees, contractors, researchers, students, volunteers, representatives of Federal, state, local, or tribal agencies, and any others not specifically mentioned in this list) involved in, or in support of, the ISCM program as it relates to the utilization of Pondera FDaaS services.
- (2) The requirements for ISCM apply to information systems used or operated by or on behalf of Pondera Solutions and could include non-Pondera owned systems storing or processing Pondera Solutions data.

(3) Failure to maintain compliance with ISCM requirements described in this DUA Appendix document could result in denial or revocation of an End-User's authorization to use Pondera FDaaS services.

(4) Failure to maintain compliance with ISCM requirements described in this DUA Appendix document could result in denial or revocation of an client organizations' authorization to use Pondera FDaaS services.

## Assumptions

These processes and procedures assume that:

- (1) All requisite security and privacy training required for system access has been successfully provided to the End User and is formally documented.
- (2) That all End User License Agreements (EULAs) for End Users and End User Administrators have been understood and signed by authorized Client Administrative personnel and each End User.
- (3) Client Administrative personnel have been educated on, and agree to, any required event escalation process for security or privacy matters.
- (4) FDaaS system and service access has been configured in accordance with the End User's authorization profile.

## **Auditing Processes and Procedures**

### **Initial Audit and Monitoring Process for new End Users**

New End Users must be audited for compliance with service usage constraints. Within 90 calendar days from the activation of a New User's FDaaS access credentials, the Pondera CSO will:

- (1) Create an extract report (End User Activity Report) from the FDaaS system detailing the FDaaS function and data utilization profile of the End User inclusive of the date and time of:
  - a. All major FDaaS functionality exercised by the End User
  - b. All queries made to, or usage of Third-Party data sources
- (2) Deliver the End User Activity Report to the End User Client Administrator (or designated alternate representative) familiar with legitimate End User assignments and capable of identifying non-sanctioned system or data utilization. The report will be provided in a form consistent with specific audit requirements and agreements.
- (3) Collect and maintain the results of Client Administrator review of End User Activity Reports for a minimum of five (5) years, unless stipulated by contract for a different time period, or associated with contract termination requirements.
- (4) Auditing Log Data maintained by Pondera will be purged on a periodic basis in accordance contractual requirements.

### **Periodic Monitoring and Re-Evaluation**

Pondera coordinates with client representatives to repeat steps 1-3 above every 90 days, for each and every End User, from the date of the initial User Activity Report, for the duration of the End Users' authorized access to FDaaS services.

### **Randomized Monitoring and Evaluation**

Within every 90 calendar day period from the date of activation of any new FDaaS access by any client organization, the Pondera CSO will:

- (1) Create an extract report (End User Activity Report) from the FDaaS system detailing the FDaaS function and data utilization profile of, at least, twenty (20) percent of the End User individuals associated with the End User organization. The selection of the candidate End Users to be audited, will be randomized (the algorithm will not be discussed within the context of this document). The End User Activity Report will include the date and time of:
  - a. All major FDaaS functionality exercised by the End User(s)
  - b. All queries made to, or usage of Third-Party data sources
- (2) Deliver the End User Activity Report to the End User Client Administrator (or designated alternate representative) familiar with legitimate End User assignments and capable of identifying non-sanctioned system or data utilization.
- (3) Collect and maintain results of Client Administrator review of End User Activity Reports for a minimum of five (5) years.

## Purging of Data

Under default circumstances, the Pondera CSO will collect and maintain the results End User activity analysis reports for a minimum of five (5) years, unless stipulated by contract for a different time period, or associated with contract termination requirements.

Auditing Log Data will be purged using industry standard data destruction technique after a period of five (5) years, unless stipulated by contract for a different time period, or associated with contract termination requirements.