STATE OF CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

CONTRACT TRANSACTION REQUEST (Internal)

If requested, return material to:
Contracts and Purchasing Bureau
M.S. 8-14-747

DATE	AGREEMENT NUMBER
4/9/15	**15-MOU-00576**

☒ **Division: Administration Division**
Program: Child Welfare Data Analysis Bureau
Attn: Fran Mason
Mail Station: 19-13-84
☐ **Budget Bureau**
☐ **Performance Monitoring and Research Bureau**

☐ M.S. 9-4-71, **Fiscal Systems**
☐ M.S. 9-4-72, **Fund Acct and Rept. (Enc)**
☐ M.S. 9-4-72, **Fund Acct. and Rept. (Rec)**
☐ M.S. 9-5-84, **Financial Services (Pay)**
☐ **Information Security Officer**

☐ M.S. 8-5-161, **LEGAL**
☐ **PEER REVIEW**
☐ Other: M.S.

CONTRACTOR NAME	TERM
California Department of Health Care Services	From: **Upon approval** Through: **Until cancelled**

PURPOSE	TYPE OF DOCUMENT
Agreement for the exchange of data between CDSS, DHCS and agreed counties and tribes. Global MOU Child Welfare Services.	**Memorandum of Understanding**

ACCOUNT TYPE	AMOUNT	INDEX CODE	FUNDING TYPE	FUNDING SOURCE	PCA
☐ Payable ☐ Receivable	**$0.00**	**N/A**		☐ Federal ☐ State	**N/A**

CONTRACT OFFICER	TELEPHONE	FAX NUMBER
Rosa Sanchez	**(916) 657-2364**	**(916) 657-2362**

☐ Please review and comment on the attached proposed Agreement or amendment, sign below, and return by
☐ Please forward a Board Resolution. Contracts in excess of $5,000 by State Boards must be accompanied by a copy of the resolution authorizing the Agreement.
☐ Please encumber funds for the attached Agreement and return to the Contracts and Purchasing Bureau.
☒ We are forwarding a copy of the fully executed Agreement.
- ☐ Requestor is responsible for approving the appropriate expenditures within contract limitations, ensuring contractor compliance with contractor responsibilities as identified in the attached contract, and distributing all progress and final reports. Contract irregularities are to be reported to the Contracts and Purchasing Bureau.
- ☐ Requestor is responsible for evaluating contractor's performance for compliance with the terms of the contract within 60 days after completion of the contract. The attached STD 4, Contract/Contractor Evaluation, must be completed and submitted to the Contracts and Purchasing Bureau before .
- ☐ Requestor must notify the Business Services Bureau, Safety/Security Section of contractors providing on-site service at 744 P Street.

☐ The contract has been terminated. Please disencumber funds effective .
☐ The pending contract has been canceled. The cancellation was authorized by .
☐ Other: .

REVIEWER COMMENTS/SIGNATURE:

☐ Acceptable as is.
☐ Acceptable with revisions. See attached marked up contract.
☐ No impact on my area of responsibilities.

SIGNATURE (Bureau Chief or above)	BUREAU	DATE

ENCUMBRANCE INFORMATION

FISCAL YEAR	INDEX	OBJECT	AGENCY	PCA / AMOUNT	CFDA #

IF FEDERALLY FUNDED, PROVIDE THE FOLLOWING INFORMATION:

CFDA TITLE	CFDA NUMBER	AWARD NAME	AWARD NUMBER	AWARD YEAR	NAME OF FEDERAL AGENCY	R& D (Y or N)

GLOBAL MEMORANDUM OF UNDERSTANDING
CHILD WELFARE SERVICES

I. RECITALS

This Memorandum of Understanding (MOU) is entered into by and between the California Department of Social Services (CDSS), the California Department of Health Care Services (DHCS), and those California Counties and Title IV-E Tribes that have agreed to the terms and conditions of this MOU by becoming signatories to this MOU (hereafter "parties"); to set forth the terms and conditions for the exchange of confidential data, collected and retained by CDSS and DHCS (Department(s)), for the purpose of matching the confidential data, hereinafter referred to as 'matched data,' to administer and implement the applicable federal and/or state health and public social service programs described herein. This MOU also sets forth the terms and conditions imposed on each Department, when it is necessary for program purposes, to share identifiable and de-identified matched data with signatory California counties and Title IV-E Tribes (hereafter "counties or tribes"), authorized entities and de-identified data with the public.

CDSS and DHCS, pursuant to Welfare and Institutions Code (WIC), Division 9, § 10000 *et seq*., are responsible for the administration and delivery of public social services.

WIC § 10051 defines 'public social services' as:

> "…activities and functions of state and local government administered or supervised by the department or the State Department of Health Services and involved in providing aid or services or both, including health care services and medical assistance, to those people of the state who, because of their economic circumstances or social conditions, are in need thereof and may benefit thereby."

Specifically, CDSS is the single state agency under Title IV of the Social Security Act that is responsible for oversight of county and community agencies in the implementation of child welfare services programs which includes services for children in foster care and other services provided on behalf of children who are or are alleged to be the victims of child abuse, neglect, or exploitation. CDSS responsibilities include, but are not limited to, implementing the state Health Care Oversight Plan under Title IV-B and IV-E to ensure that the physical and mental health needs of children in foster care are identified and met. Pursuant to WIC § 10850, CDSS is authorized to provide confidential data to county public agencies, private agencies, and Native American tribes with a Title IV-E agreement pursuant to WIC § 10553.1 (hereinafter Title IV-E tribe) that are directly connected with the administration of these programs by providing, or securing, public social services, for or on behalf of applicants or recipients.

Specifically, DHCS is the single state agency under Title XIX of the Social Security Act that is responsible for operating and overseeing the federal Medicaid program in California, hereafter referred to as Medi-Cal. DHCS responsibilities, include, but are not limited to, ensuring high-quality and efficient health care services are provided to Medi-Cal beneficiaries, which categorically include children in foster care and former foster youth who attain age 18 while in a foster care placement. Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), DHCS is authorized to provide and exchange protected health information (PHI) of an individual for the purposes of treatment, payment, and health care operations (See 45 CFR § 164.502). Health care operations includes: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance

activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities (See 45 CFR§ 164.501).

Specifically, pursuant to WIC §10800, the counties are responsible for the administration and provision of public social services, including child welfare services, in each county of the state. The provision of public social services in the counties must comply with state and federal laws including the regulations of the CDSS and DHCS. Further, Title IV-E tribes, through their agreements with either the State or directly with the federal government, are responsible for ensuring the health and safety of children or non-minor dependents receiving child welfare services under the jurisdiction of the tribe.

Based on the federal and state authority of each Department, the obligation of the counties and Title IV-E tribes to administer public social services, and for the purpose of complying with each Department's respective and mutual responsibilities and requirements as it pertains to children or non-minor dependents receiving child welfare services and former foster youth, the parties hereby agree to the following terms and conditions in the exchange of confidential data and use of matched confidential data.

II. PURPOSE

The parties agree to the exchange of both confidential and non-confidential data. The use and disclosure of such data shall be limited to the following purposes:

1. Analysis and reporting for the purposes set forth in 42 USC § 622(b)(15) which includes, but is not limited to:

    a) Ongoing oversight of health care services for any children or non-minor dependents receiving child welfare services;

    b) Ensuring a coordinated strategy to identify and respond to the health care needs of children or non-minor dependents receiving child welfare services; and

    c) Ensuring Medi-Cal enrollment for former foster youth up to age 26 and, through data sharing, facilitating the extension of Medi-Cal enrollment of existing foster care youth up to age 26 as they exit the program.

2. Analysis, reporting, and auditing to provide ongoing administration, operation oversight, coordination, program monitoring, and evaluation of health treatment, including mental health services and pharmaceutical services to children or non-minor dependents receiving child welfare services.

3. Reporting federal Adoption and Foster Care Analysis and Reporting System (AFCARS) data elements as described per § 479 of the Social Security Act and 45 CFR § 1355.

4. To share amongst the parties, as applicable and appropriate, matched data containing confidential information and de-identified data, reports and analyses based upon matched data to support the administration and provision of public social services to children or non-minor dependents receiving child welfare services.

III. DEFINITIONS

"Breach" shall have the meaning given to such term under HIPAA and the HIPAA regulations and includes any known or suspected information security incidents (intentional or unintentional, that cause or may cause loss, damage, destruction, misuse, or unauthorized disclosure of information, as provided in the Social Security Administration Information Exchange Agreement (SSA IEA)); the CDSS Confidentiality and Security Requirements for California State Agencies; and the California Information Practices Act.

"Children or non-minor dependents receiving child welfare services" means children or non-minor dependents on whose behalf the county child welfare agency or probation department is providing child welfare services as described in WIC § 16501(a). This includes, but is not limited to, the following:

1. Children and non-minor dependents who are dependents of the juvenile court or are receiving voluntary child welfare services.
2. Children and non-minor dependents who are wards of the juvenile court and are in a foster care placement.
3. Children and non-minor dependents who are receiving child welfare services provided by a tribe with a Title IV-E agreement.

"Confidential data" means Information that identifies or is substantially likely to identify an individual and that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or has restrictions on disclosure in accordance with other applicable state or federal laws, including but not limited to WIC 10850. As used in this MOU Confidential data may include Protected Health Information (PHI), or Individually Identifiable Health Information as defined in HIPAA, 45 CFR 160.103; or "Limited data set (LDS)" as defined in 45 CFR 164.514; or Personal Information (PI), as defined in California Civil Code, §§ 1798.3, 1798.24 and 1798.29; or Personally Identifiable Information (PII), as defined in the Social Security Administration Information Exchange Agreement (SSA IEA) and DHCS Business Associate Addendum (BAA).

"Counties" means the largest political subdivision of the State having corporate powers (Govt. Code section 23000). As used in this MOU counties refers to the current 58 counties of California.

"Data" is a representation of facts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automated means. As used in this MOU data would refer to information related to children receiving child welfare services or non-minor dependents or former foster youth.

"Alcohol and Drug Abuse Patient Records data" covered by 42 CFR Part 2, is excluded from this MOU.

"De-identified data" means information that does not identify an individual such that there is no reasonable basis to believe that the information provided can be used to identify an individual. HIPAA provides that data can be considered de-identified if a person experienced in statistical methods for rendering information not identifiable determines the risk is small that the information could be used to identify an individual or specific identifiers identified in the HIPAA regulations are removed (45 CFR 164.514(a) and (b)(1) or (b)(2)). De-identified data is not PHI.

"Department(s)" means the California Department of Social Services and/or the California Department of Health Care Services.

"Former Foster Youth" means a former non-minor dependent, as defined by WIC § 11400(v), who was in foster care on his or her 18th birthday and is under the age of 26 at the time of any request for data, regardless of whether the youth is receiving any child welfare service.

"Matched data" means the combining of confidential health and child welfare services information from a covered entity to a business associate for analyses and use that relates to the health care and child welfare services operations of the respective entities (also known as data aggregation under 45 CFR 164.501).

"Personal Information" (PI) means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual." (CA Civil Code section 1798.3)

"Personally Identifiable Information" (PII) is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data. (Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, ver. 6.0.2, (April 2014) p. 9)

"Protected Health Information" (PHI) means individually identifiable health information. (45 CFR 160.103).

"Security Incident" means any event (intentional or unintentional) that causes the loss, damage to, destruction, misuse or unauthorized disclosure of CDSS/DHCS information assets.

"Use" means the sharing, employment, application, utilization, examination or analysis of data. (45 CFR 160.103).

IV. CONFIDENTIAL DATA REQUESTS

A. Identification of Confidential Data

The parties agree to identify and share with each other data which is collected and retained by each party pertaining to children or non-minor dependents receiving or previously receiving child welfare services. The only data exchanged will be for the stated purposes in section II, in order to comply with HIPAA. Data will include, but not be limited to, the following categories of information:

- Eligibility Data,
- Demographic Data,
- Social Services Data,
- Medical Data,
- Mental Health Data, and
- Payment Data.

B. Tracking Process for Exchange of Data

Within 30 days of the execution of this MOU, CDSS and DHCS shall develop, following consultation with counties and tribes, and agree upon a written request and response process for the exchange of data between the parties. This process shall include a tracking system for logging each data request, extract, exchange, and match, as applicable. Development and agreement regarding this process shall not forestall data sharing consistent with the terms of this MOU in advance of that process; however, formal record of such data sharing shall be made pursuant to the process once the process has been agreed upon.

At the time of a request for data, the applicable parties shall mutually assess and agree upon the purpose of the data and the intended retention period for the data based upon its purpose and use by the parties. At the expiration of the agreed upon purpose for the data and matched data sets the data shall be returned or destroyed pursuant to the HIPAA Business Associate Addendum (Exhibit A) and the CDSS Confidentiality and Security Requirements (Exhibit C) unless the parties mutually agree in writing to a new purpose and retention period for the data and matched data sets. At minimum, the tracking system shall include:

1. Identification of the individual(s) responsible in each party to receive data and data requests, authorize the exchange or provision of data for his/her party, and be responsible for providing the requested data to the other party.

2. A log that tracks each data set requested, extracted, exchanged and/or matched, under this MOU. The log must include, at a minimum, the following about the data to be exchanged:

    a) Data elements;
    b) Population;
    c) Relevant time period;
    d) Purpose;
    e) Request date;
    f) Delivery date;
    g) Retention period;
    h) Frequency of data provision;
    i) Authority; and
    j) Person who reviewed and authorized the release, pursuant to the written request.

C. Process for Requesting Data and Matched Data

1. The requesting party shall provide to the providing party's Project Representative identified pursuant to Section B(1) of this MOU a written request for data and/or matched data using prescribed formats and following the agreed upon data request process. The written request shall describe the information requested, including but not limited to the purpose and intended use of the requested data; the authority for the intended use of the data; how the intended use is in accordance with the purposes of this MOU; and who the intended users are.

2. The request shall also include information regarding the following:

    a) Population;
    b) Relevant time period;
    c) Request date;
    d) Delivery date;
    e) Retention period; and
    f) Frequency of data provision;

    Upon receipt of the written request, the applicable parties will evaluate the request for completeness, for compliance with this MOU and applicable laws. Requests shall be prioritized, if necessary, at the sole discretion of the data owner, although reasonable effort shall be made to accommodate the needs of the requesting party. If the data or matched data will be provided by the DHCS or CDSS to a county or tribe, then CDSS will coordinate the planning, format, and delivery with the requesting party.

D. Data Sharing between the Parties in Compliance With All Applicable Laws

1. Each party shall be responsible for ensuring that any data that is shared, matched, exchanged or used is done so in compliance with all applicable state and federal laws.

2. When CDSS is accessing or using confidential data provided by DHCS, CDSS agrees to comply with the provisions of the DHCS HIPAA Business Associate Addendum (Exhibit A), the IEA SSA and DHCS Agreement (Exhibit B.1), attached to this MOU and all Federal and State privacy and security laws.

3. When DHCS is accessing and using confidential data provided by CDSS, DHCS agrees to comply with the provisions of the CDSS Confidentiality and Security Requirements for California State Agencies (Exhibit C), the IEA SSA and CDSS Agreement (Exhibit B.2), and all Federal and State privacy and security laws.

4. Matched confidential data furnished by CDSS and/or DHCS that is transmitted to other parties to this MOU is subject to the DHCS HIPAA Business Associate Addendum (Exhibit A), CDSS Confidentiality and Security Requirements (Exhibit C), the SSA agreements, (Exhibits B.1 and B.2), and all federal and state privacy and security laws.

5. Matched confidential data furnished by any party pursuant to this MOU will be used or disclosed only as specifically provided by this MOU. Matched confidential data furnished by any party pursuant to this MOU shall not be disclosed for use to any person other than the authorized parties' staff who is assigned to the use the data for the purposes authorized under this MOU.

6. Each party shall maintain a written record of staff authorized to access and who have accessed (users) the confidential data that has been exchanged pursuant to this MOU. Each party shall provide a copy of its users that have accessed the confidential data provided pursuant to this MOU, to other parties upon request.

7. Pursuant to this MOU and for purposes of their respective program responsibilities, either party may transmit confidential data, matched data sets, and reports regarding children or non-minor dependents receiving child welfare services. Data and matched datasets containing confidential data may be shared only for purposes directly connected with the administration of child welfare services or health care services.

When transmitting confidential data to another party, both the sending and receiving party shall comply with all appropriate privacy and security requirements and procedures, including the use of encryption.

E. Data Sharing Activities

The parties shall mutually engage in the following activities to support the data sharing between the parties authorized by this MOU by:

1. Participating in the planning and design of the exchange of data.

2. Providing access to completed data extracts and matches, in a manner and at a time mutually agreed upon.

3. Requesting additional information from the data extracts and matched data sets, as needed by either party for administrative purposes, including verifying and tracking the provision of information or services to applicants for and recipients of programs.

F. Breach Response Process by the Parties for Matched Data

1. The party in possession of the data when the breach occurs and who experiences the breach will be responsible for reporting to all pertinent parties, for complying with all applicable laws, and for all costs and liabilities related to the breach.

2. If CDSS is responsible for a breach, CDSS will report the breach to and comply with DHCS HIPAA Business Associate Addendum (Exhibit A) and the DHCS' SSA agreement (Exhibit B.1).

3. If DHCS is responsible for the breach of CDSS provided data, DHCS will report the breach to and comply with CDSS' Confidentiality and Security Requirements (Exhibit C) and the CDSS SSA agreement (Exhibit B.2).

4. If a county or tribe is responsible for the breach, the county or tribe will be responsible for the breach notifications and reporting the breach to CDSS and DHCS as set forth in the DHCS HIPAA Business Associate Addendum, (Exhibit A); the CDSS Confidentiality and Security Requirements (Exhibit C), and the SSA agreements, (Exhibits B.1 and B.2).

5. The persons to be notified and the process for notice in the event of a breach are identified in the DHCS HIPAA Business Associate Addendum (Exhibit A) and CDSS Confidentiality and Security Requirements (Exhibit C) except that the contact information for CDSS and DHCS are:

Nola Niegel
Acting Information Security Officer
Information Systems Division
California Department of Social Services
744 P Street, M.S. 9-9-70
Sacramento, CA 95814
(916) 654-0694
iso@dss.ca.gov

DHCS Privacy Officer	DHCS Information Security Officer
Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874

V. RESPONSIBILITIES FOR DATA DISSEMINATION OUTSIDE OF THE PARTIES OF THE MOU

A. De-identified Data Released to Entities Outside of the Parties

De-identified data or reports containing only de-identified data provided pursuant this MOU to the parties may be transmitted to outside parties. Data shall be de-identified in compliance with HIPAA and other applicable laws and regulations, and the process for de-identification of data provided herein.

B. Data Sharing by Parties with Authorized Entities or Contractors

Parties to this MOU may provide confidential or de-identified data, including matched data, to authorized entities or contractors that have contracted with the parties for the provision of program services to children or non-minor dependents receiving child welfare services if the parties have determined that it is necessary for their ongoing, administration, oversight, monitoring, evaluation, and reporting responsibilities. All such contracts must include the Exhibits to this MOU. All data provided to authorized entities or contractors shall meet the minimum necessary requirements of HIPAA.

C. Articles for Publication

1. CDSS/DHCS

CDSS and DHCS may participate in the writing and reviewing of each other's reports and articles that refer to or include information regarding the subject matters of this MOU that are intended for publication. For the purpose of this MOU, publication means that an article or report is intended to be provided or made available to the general public. This includes posting reports, articles or data on the Internet or in any other public medium or forum. Only de-identified information as defined by HIPAA shall be used for publishing reports and/or articles that may or are made available to the public. The process for de-identified data provided herein shall be used by the departments for reaching mutual agreement on articles and reports for publication. This paragraph does not apply, and mutual agreement by CDSS and DHCS is not required, for reports (such

as outcome measures) that are produced by CDSS or DHCS in the ordinary course of the operation or administration of their own programs using only data in their respective systems.

2. County or Tribe

Matched confidential data released to counties shall not be used for publications produced by the counties or tribes. Only de-identified information as defined by HIPAA shall be used for publishing reports and/or articles that may or are made available to the public.

D. Other Special Reports and Analyses by the Parties

The parties may develop other special reports such as regional/geographic analyses, demographic variations, and so forth under this MOU for each party's internal use. Only de-identified data shall be included in any published analyses or reports.

E. Process for De-identification

1. CDSS/DHCS

Each Department is responsible for determining the sufficiency of the HIPAA de-identification determination for its intended use of the de-identified data by the Department. Prior to implementing the intended use of the de-identified data each Department agrees to provide to the other Department for review, the proposed de-identified data to be used. If the reviewing Department disagrees with the de-identification determination that has occurred, the reviewing Department shall notify the Department of its assessment and objections within five working days of receiving the de-identified data. If the Departments cannot agree within 10 working days following the notification of objections to the de-identified data, the matter shall immediately be referred to the first level of the Dispute Resolution Process using the Form, Exhibit D.

2. County or Tribe

Each county or tribe is responsible for determining the sufficiency of the HIPAA de-identification determination for its intended use of the de-identified data by the county or tribe. Prior to the intended use of the de-identified data the county or tribe agrees to provide to the Departments relevant information related to the de-identification. If either of the Departments disagrees with the de-identification determination of the county or tribe that has occurred and the parties cannot agree within 10 working days, the matter shall immediately be referred to the first level of the County or Tribe Dispute Resolution Process using the Form, Exhibit D.

F. Miscellaneous Requests for Data – PRA

1. CDSS/DHCS

In the event either Department receives a Public Records Act (PRA) request, a subpoena, litigation-related request, or any other request for the confidential information that is the subject of this MOU and not otherwise provided for herein, the Department receiving the request shall immediately notify the other Department and meet and confer as necessary on the appropriate response to the request.

2. County or Tribe

In the event that a County or Tribe receives a Public Records Act (PRA) request, a subpoena, litigation-related request, or any other request for the confidential information that is the subject of this MOU and not otherwise provided for herein, the county or tribe shall immediately notify the Project Representatives of both Departments and meet and confer as necessary on the appropriate response to the request.

G. Consent - CDSS/DHCS

If any issues of whether consent is needed from children or non-minor dependents receiving child welfare services before confidential data can be used or shared with third parties for the purposes of this MOU, DHCS and CDSS agree to meet and confer, and within 30 days to mutually agree, on a form or process for gaining the consent of the children or non-minor dependents receiving child welfare services or the child's representative.

H. Existing Data Use Agreements Between CDSS and DHCS

At the time of the execution of this MOU, there are existing data use agreements between CDSS and DHCS directly related to the purposes of this MOU. These existing agreements shall continue in full force and effect until their expiration, at which time their purposes and provisions shall be incorporated into and made a part of this MOU as though fully set forth herein.

VI. TERM

A. CDSS/DHCS

The term of this MOU shall commence upon the approval and signature of the Director of both Departments and shall continue in effect until cancelled by either Department. Written notice of cancellation shall be provided by the cancelling Department to the other Department no later than 180 days prior to the specified cancellation date.

B. County or Tribe

The term of this MOU with each county or tribe shall commence upon the approval and signature of the County or Tribe and continue in effect until cancelled by the Departments or County or Tribe. Written notice of cancellation shall be provided by the cancelling party to the Department(s), county or tribe or by the Department(s) to the county or tribe no later than 180 days prior to the specified cancellation date.

VII. PAYMENT

There is no compensation payable to any of the parties in connection with this MOU.

VIII. AMENDMENT PROCESS

A. Non-Substantive Changes by the Parties

Any party may propose written non-substantive changes or revisions to the information, activities and tasks of this MOU without amendment provided such changes do not alter the

overall goals and basic purpose of the MOU. The changes will be effective upon the mutual agreement of the affected parties. The addition of individual Counties or Tribes to this MOU, as provided herein, shall be a non-substantive change and shall not require a formal amendment.

B. Substantive Changes by the Parties

A party, during the term of this MOU, may propose a substantive change or amendment to the terms of this MOU. Such changes or amendments shall be proposed in writing to the other parties, and the parties agree to meet and confer within 10 working days to discuss or negotiate the proposed changes. The agreed-upon changes to this MOU shall be made through an expedited amendment process that will be reviewed and approved by each party's executive, program and legal staff and signed by the party's Director or designee. The expedited amendment will be completed and processed within 30 days unless this time is extended by the parties. This expedited amendment shall be binding on all parties upon the approval and signature of the parties' Directors or their designee.

IX. DISPUTE RESOLUTION PROCESS

A. CDSS/DHCS

If a dispute arises between DHCS and CDSS, the Departments must seek resolution using the process outlined below.

1. The aggrieved department should first informally discuss the problem with the Project Representative and Contract Manager of the other Department. If the problem cannot be resolved informally, the aggrieved Department must direct the grievance together with any evidence, in writing, to the Chief Deputy Director of the other department. The grievance must state the issues in dispute, the legal authority or other basis for the Department's position and the remedy sought. The Chief Deputy Director must render a decision within ten (10) working days after receipt of the written grievance. The Chief Deputy Director shall respond in writing to the aggrieved Department indicating his/her decision and the reason(s) therefore. Should the aggrieved Department disagree with the Chief Deputy Director's decision, the aggrieved Department may appeal to the second level.

2. When appealing to the second level the aggrieved Department must prepare an appeal indicating the reasons for disagreement with the Chief Deputy Director's decision. The aggrieved Department shall include with its appeal a copy of its original statement of dispute along with any supporting evidence and a copy of the Chief Deputy Director's decision. The appeal shall be addressed to the Health and Human Services Agency (HHSA) Secretary or his/her designee within ten (10) working days from receipt of the Chief Deputy Director's decision. The HHSA Secretary or his/her designee shall meet with the aggrieved Department to review the issues raised. A written decision signed by the HHSA Agency Secretary or his/her designee shall be directed to the aggrieved Department within twenty (20) working days of receipt of the second level appeal.

B. County or Tribe

If a dispute arises between the Departments and a County or Tribe, the County or Tribe must seek resolution using the process outlined below.

1. The aggrieved party should first informally discuss the problem with the Project Representative and Contract Manager of the other party. If the problem cannot be resolved informally, the aggrieved party must direct the grievance together with any evidence, in writing, to the Program Branch Chief of the Project Representative for Department(s) or designee for the Tribe or County, as applicable. The grievance must state the issues in dispute, the legal authority or other basis for the party's position and the remedy sought. The party receiving the grievance must render a decision within ten (10) working days after receipt of the written grievance of the other party. The grievance shall be responded to in writing to the aggrieved party indicating their decision and reasons therefore. Should the aggrieved party disagree with the decision, the aggrieved party may appeal to the second level.

2. When appealing to the second level the aggrieved party must prepare an appeal indicating the reasons for disagreement with the decision by the other party. The aggrieved party shall include with its appeal a copy of their original statement of dispute along with any supporting evidence and a copy of the prior decision of the other party. The aggrieved party shall address the appeal to the other party's second level appeal designee within ten (10) working days from receipt of the written decision of the other party. (For the Departments the second level appeal designee will be the Deputy Director of the division in which the branch is organized, or his/her designee; for the County or Tribe the second level appeal will be to the County or Tribes designee.) The second level appeal designee shall meet with the aggrieved party to review the issues raised. A written decision signed by the second level appeal designee shall be directed to the aggrieved party within twenty (20) working days of receipt of the second level appeal.

X. SURVIVAL

The privacy, confidentiality, and security provisions of this MOU survive the termination or expiration of this MOU.

XI. INCORPORATED EXHIBITS

The following exhibits are incorporated herein, and made a part hereof by this reference:

1) Exhibit A	HIPAA Business Associate Addendum	15 pages
2) Exhibit B.1	IEA SSA and DHCS Agreement	74 pages
3) Exhibit B.2	IEA SSA and CDSS Agreement	77 pages
4) Exhibit C	CDSS Confidentiality and Security Requirements for California State Agencies	6 pages
5) Exhibit D	Form for Dispute Resolution	1 page

XII. PROJECT REPRESENTATIVES AND SIGNATORIES

The project representatives during the term of this MOU from the California Department of Social Services will be:

Project Representative	Contract Manager
Akhtar Khan Branch Chief or designee Research Services Branch (916) 653-1800 Akhtar.Khan@dss.ca.gov	Alicia Sandoval Child Welfare and Data Analysis Bureau Research Services Branch (916) 653-1812 Alicia.Sandoval@dss.ca.gov

The project representatives during the term of this MOU from the California Department of Health Care Services will be:

Project Representative	Contract Manager
Linette Scott Deputy Director or designee Information Management Division (916) 440-7639 Linette.Scott@dhcs.ca.gov	Angelique Lastinger Information Management Division (916) 332-8573 Angelique.Lastinger@dhcs.ca.gov

Either department may make changes to the project representatives above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement. Each County or Tribe signing this MOU will designate and identify to the Departments the Project Representative for the County or Tribe that will be the single point of contact with the Departments for County or Tribe to receive and make requests for data to the Departments.

XIII. COUNTY AND TRIBE - PROJECT REPRESENTATIVES AND SIGNATORIES

By signing this MOU, the County or Tribe signatory represents that he or she has authority to bind and obligate the specific County or Tribe the signatory represents. On behalf of the County or Tribe the signatory agrees to the terms, conditions and obligations of this MOU including but not limited to ensuring the integrity, security, and confidentiality of all data provided by the Departments. In addition, the signatory is responsible for permitting disclosure or any distributions of the data to other County or Tribe entities or users and to permit only those disclosures and uses that are consistent with this MOU and as permitted by law.

This Memorandum of Understanding is not effective until signed by all parties.

California Department of Social Services

By: _____ Date: 4/8/15
Will Lightbourne, Director

California Department of Health Care Services

By: _____ Date: 4/8/15
Jennifer Kent, Director

SIGNATURE PAGE FOR COUNTY

This Memorandum of Understanding is not effective until signed by all parties.

By: _____ Date: _____

SIGNATURE PAGE FOR TRIBE

This Memorandum of Understanding is not effective until signed by all parties.

By: _____ Date: _____

Exhibit A
HIPAA Business Associate Addendum

I. Recitals

A. This Contract (Agreement) has been determined to constitute a business associate relationship under 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 ('the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 (“the HIPAA regulations”).

B. The Department of Health Care Services (“DHCS”) wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information (“PHI”), including protected health information in electronic media (“ePHI”), under federal law, and personal information ("PI") under state law.

C. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties.”

D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that DHCS must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and 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.

E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

II. Definitions

A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.

B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.

C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule.

D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.

Exhibit A
HIPAA Business Associate Addendum

E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

F. 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.

G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.

H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.

I. Protected Health Information 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.

J. 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.

K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.

L. 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 Business Associate’s organization and intended for internal use; or interference with system operations in an information system.

M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act, and the HIPAA regulations.

III. Terms of Agreement

A. Permitted Uses and Disclosures of PHI by Business Associate

Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the

Exhibit A
HIPAA Business Associate Addendum

HIPAA regulations, if done by DHCS. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2.

1. ***Specific Use and Disclosure Provisions***. Except as otherwise indicated in this Addendum, Business Associate may:

   a. ***Use and disclose for management and administration***. Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

   b. ***Provision of Data Aggregation Services***. Use PHI to provide data aggregation services to DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of DHCS.

B. Prohibited Uses and Disclosures

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).

2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of DHCS and as permitted by 42 U.S.C. section 17935(d)(2).

C. Responsibilities of Business Associate

Business Associate agrees:

1. ***Nondisclosure***. Not to use or disclose Protected Health Information (PHI) other than as permitted or required by this Agreement or as required by law.

2. ***Safeguards***. To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate 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 Business Associate's operations and the nature and scope of its activities, and

Exhibit A
HIPAA Business Associate Addendum

which incorporates the requirements of section 3, Security, below. Business Associate will provide DHCS with its current and updated policies.

3. ***Security***. To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

   a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;

   b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement;

   c. Providing 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; and

   d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

   Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with DHCS.

D. ***Mitigation of Harmful Effects***. 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 or its subcontractors in violation of the requirements of this Addendum.

E. ***Business Associate's Agents and Subcontractors***.

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of DHCS, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act the HIPAA regulations, and the Final Omnibus Rule, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business associates are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.

Exhibit A
HIPAA Business Associate Addendum

2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:

   a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; or

   b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

F. ***Availability of Information to DHCS and Individuals***. To provide access and information:

1. To provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable DHCS to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).

3. If Business Associate receives data from DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

G. ***Amendment of PHI.*** To make any amendment(s) to PHI that DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by DHCS.

H. ***Internal Practices***. To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.

Exhibit A
HIPAA Business Associate Addendum

I. ***Documentation of Disclosures***. To document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for DHCS as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for DHCS after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

J. ***Breaches and Security Incidents.*** During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. ***Notice to DHCS.*** (1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

   Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link:
   http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

   Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

   a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

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

Exhibit A
HIPAA Business Associate Addendum

2. ***Investigation and Investigation Report.*** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. If the initial report did not include all of the requested information marked with an asterisk, then within 72 hours of the discovery, Business Associate shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:

3. ***Complete Report.*** To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve or disapprove the determination of whether a breach occurred, is reportable to the appropriate entities, if individual notifications are required, and the corrective action plan.

4. ***Notification of Individuals.*** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer 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 of Breaches.*** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to Business Associate, Business Associate shall notify DHCS, and DHCS and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.

6. ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to

Exhibit A
HIPAA Business Associate Addendum

the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874

K. ***Termination of Agreement.*** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by DHCS of this Addendum, it shall take the following steps:

1. Provide an opportunity for DHCS to cure the breach or end the violation and terminate the Agreement if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or
2. Immediately terminate the Agreement if DHCS has breached a material term of the Addendum and cure is not possible.

L. ***Due Diligence.*** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

M. ***Sanctions and/or Penalties***. Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

IV. Obligations of DHCS

DHCS agrees to:

A. ***Notice of Privacy Practices***. Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx or the DHCS website at www.dhcs.ca.gov (select “Privacy in the left column and “Notice of Privacy Practices” on the right side of the page).

B. ***Permission by Individuals for Use and Disclosure of PHI***. Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate’s permitted or required uses and disclosures.

Exhibit A
HIPAA Business Associate Addendum

C. ***Notification of Restrictions***. Notify the Business Associate of any restriction to the use or disclosure of PHI that DHCS has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. ***Requests Conflicting with HIPAA Rules***. Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by DHCS.

V. Audits, Inspection and Enforcement

A. From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum 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, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':

1. Failure to detect or

2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' enforcement rights under this Agreement and this Addendum.

B. If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify DHCS and provide DHCS with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

VI. Termination

A. ***Term.*** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the contract and shall terminate when all the PHI provided by DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, is destroyed or returned to DHCS, in accordance with 45 CFR 164.504(e)(2)(ii)(I).

B. ***Termination for Cause***. In accordance with 45 CFR section 164.504(e)(1)(ii), upon DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by DHCS; or

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.

Exhibit A
HIPAA Business Associate Addendum

C. ***Judicial or Administrative Proceedings***. Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.

D. ***Effect of Termination***. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

VII. Miscellaneous Provisions

A. ***Disclaimer***. DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

B. ***Amendment***. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon DHCS' request, Business Associate agrees to promptly enter into negotiations with DHCS concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. DHCS may terminate this Agreement upon thirty (30) days written notice in the event:

1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by DHCS pursuant to this Section; or

2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that DHCS in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

C. ***Assistance in Litigation or Administrative Proceedings***. Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

Exhibit A
HIPAA Business Associate Addendum

D. ***No Third-Party Beneficiaries***. Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

E. ***Interpretation***. The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.

F. ***Regulatory References***. A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.

G. ***Survival.*** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of this Agreement.

H. ***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.

Exhibit A
HIPAA Business Associate Addendum

Attachment A
Business Associate Data Security Requirements

I. Personnel Controls

A. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member 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.

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

C. ***Confidentiality Statement.*** All persons that will be working with DHCS PHI or PI 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 the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

D. ***Background Check.*** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

A. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

B. ***Server Security.*** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. ***Minimum Necessary.*** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. ***Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

Exhibit A
HIPAA Business Associate Addendum

E. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

G. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

H. ***Data Destruction.*** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

I. ***System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. ***Warning Banners.*** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. ***System Logging*****.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. ***Access Controls.*** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

Exhibit A
HIPAA Business Associate Addendum

M. ***Transmission encryption.*** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

N. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

A. ***System Security Review.*** All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. ***Data Backup Plan.*** Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

V. Paper Document Controls

A. ***Supervision of Data.*** DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. ***Escorting Visitors.*** Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

Exhibit A
HIPAA Business Associate Addendum

C. ***Confidential Destruction.*** DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. ***Removal of Data.*** DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

E. ***Faxing.*** Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. ***Mailing.*** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI 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 DHCS to use another method is obtained.

California Department of Social Services (CDSS)
Confidentiality and Security Requirements for
CALIFORNIA STATE AGENCIES
Interagency Agreements/Memoranda of Understanding

I. GENERAL REQUIREMENTS

A. These requirements provide a framework for maintaining the confidentiality and security of confidential data the State agency gathers or processes in the course of carrying out the terms of this agreement with CDSS. Definitions of commonly used terms are provided. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data.*

B. No exceptions from these policies shall be permitted without the explicit, prior, written approval of authorized CDSS staff. All confidentiality and security requirements, as stated in this agreement, shall be enforced and continue throughout the term of the agreement. Data protection and security plans may be required prior to receipt of confidential data.

C. In addition, the State agency will be expected to demonstrate that it has taken specific steps to ensure the data is kept secure and confidential.

II. PRIVACY, SECURITY, AND CONFIDENTIALITY

A. All confidential data made available in order to carry out this Agreement, will be protected from unauthorized use and disclosure through the observance of the same or more effective means as that required by the State Administrative Manual Sections 5300-5399, Civil Code Section 1798 et seq., Welfare and Institutions Code Section 10850, and other applicable federal and/or State laws governing individual privacy rights and data security. Upon request, CDSS reserves the right to review, and then accept security and privacy procedures that are relevant to its data.

B. The State agency is responsible for the security of the confidential data and compliance with the terms of this agreement by its employees, contractors, or sub-contractors.

III. ACCEPTABLE USE AND DISCLOSURE

A. The State agency shall not use or further disclose confidential data other than as permitted or required by this agreement.

B. The State agency shall refer any persons not included under this agreement with CDSS, to CDSS to request access to the confidential data.

C. The State agency agrees that the information obtained will be kept in the strictest confidence and shall make information available to its own employees only on a “need to know” basis. Need to know is based on those authorized employees who need information to perform their official duties in connection with the uses of the information authorized by this agreement.

IV. INFORMATION SECURITY INCIDENTS

A. Notification: The State agency shall notify the CDSS or its designated agent of any actual or attempted information security incidents, as defined below, within 24 hours of initial detection. Information security incidents shall be reported by telephone to:

Nola Niegel
Acting Information Security Officer
Information Systems Division
California Department of Social Services
744 P Street, M.S. 9-9-70
Sacramento, CA 95814
(916) 654-0694

B. Cooperation: The State agency shall cooperate in any investigations of information security incidents.

C. Isolation: The system or device affected by an information security incident, and containing CDSS confidential data, shall be removed from operation immediately to the extent necessary to prevent further harm or unauthorized disclosures. It shall remain removed from operation until correction and mitigation measures have been applied. CDSS must be contacted prior to placing the system or device, containing CDSS confidential data, back in operation. The affected system or device, containing CDSS confidential data, shall not be returned to operation until CDSS gives its approval.

V. ENCRYPTION AND TRANSMISSION

A. The State agency shall ensure the confidentiality of CDSS data transmission.

B. The State agency shall ensure that all electronic file media used in data exchanges are either:

1. Transferred by secure file transfer protocol; or

2. Encrypted or protected with equally strong measures if placed on any personal computer (either desktop or laptop), or on any removable storage media of any kind, pursuant to Budget Letter 05-32.

C. Transmission of CDSS confidential data by fax shall not be used unless no other method of transmission is feasible and with the following pre-cautions:

1. Faxes containing CDSS confidential data shall not be left unattended.

2. Fax machines shall be in secure areas.

3. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them.

4. Fax numbers shall be verified with the intended recipient before sending

D. Transfer of CDSS confidential data via paper copy shall be mailed using a secure, bonded mail service, such as Federal Express, Golden State Overnight or by registered U.S. Mail (i.e., accountable mail using restricted delivery). All packages must be double packed with a sealed envelope and a sealed outer envelope or locked box.

VI. NETWORK SECURITY

A. CDSS confidential data shall be secured against logical or physical access on any computing device, on any storage media, or in transit.

B. Maintaining a firewall separating any network attached computing device containing the data from any network not controlled by the contractor.

C. Using password based authentication and other security safeguards and precautions to restrict logical and physical access to the data to authorized users only.

D. Maintaining a log of all accesses to the data.

E. Restricting removal of the data from the work location.

F. Applying all vendor supplied security patches and updates to all computing devices containing or having access to the data.

G. Configuring all computing devices containing or having access to the data in a secure manner including:

1. Requiring the authentication or re-authentication after an established period of inactivity.

2. Not allowing remote access to CDSS confidential data or the server that stores it unless:

a. The remote computer is physically secure and located in manner to ensure the privacy of the data displayed or stored on it.

b. Communication to the server must be on a physically secured dedicated line, through a remote control solution using SSL encryption, or through a strongly encrypted VPN with firewalls that do not permit split tunneling, not on a public network.

c. The remote computer accessing CDSS data must be owned and controlled by the contractor and must not be configured in a less secure manner than the contractor’s internal computers.

VII. RETURN OR DESTRUCTION OF DATA

A. Return or Destruction: Confidential data used, compiled, processed, stored or derived by the State agency in the performance of this agreement shall be destroyed or returned by the agency. All such data shall either be returned to

CDSS in an agreed-upon format within 30 days of termination of this contract or be destroyed, unless this agreement expressly authorizes the State agency to retain specified confidential data after the termination of this agreement. If the data is returned to CDSS, the State agency shall provide CDSS with the media and an inventory of the data and files returned.

B. For purposes of this subsection, "derived" confidential data shall refer to a data set, containing confidential data, that is derived from another data set by (a) elimination of fields from the original data set, (b) addition of fields to the original data set, (c) manipulation of the structure of the original data set or a derivative data set, or (d) renaming an original data set.

C. Methods of Destruction: The State agency shall destroy all confidential data not returned when the use authorized ends in accordance with approved methods of confidential destruction (via shredding, burning, certified or witnessed destruction, or degaussing of magnetic media). All computer sets containing individual identifiers shall be destroyed. The agency shall use wipe software on all the hard drive surfaces of computers used to process or store CDSS confidential data when the computer is withdrawn from use in processing or storing such data. This includes back-up media. Destruction shall occur before the effective date of termination of this contract and a letter of confirmation shall be provided to CDSS detailing when, how, and what CDSS data was destroyed. This certification letter is required whether destruction services are contracted or the agency performs the destruction.

VIII. CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT

Based on the requirements of the Welfare and Institutions Code Section 10850, Civil Code Section 1798 et seq., and State Administrative Manual Sections 5300-5399, the State agency shall provide security sufficient to ensure protection of confidential information from improper use and disclosures, including sufficient administrative, physical, and technical safeguards to protect personal information from reasonable anticipated threats to the security or confidentiality of the information.

AGREEMENT NUMBER: _____

NAME OF STATE AGENCY: _____

**Signature of Authorized State Official*	
Title:	*Date:*
Phone: *Fax:*	*E-Mail Address:*
**Title: Information Security Officer Signature*	*Date:*
Phone: *Fax:*	*E-Mail Address:*

** Signatures are required by the Information Security Officer and Authorized State Official. This may include the Agency Chief Information Officer, System Administrator, or other individual responsible for ensuring compliance with the confidentiality and security requirements*.

IX. DEFINITIONS

For the purposes of these requirements, the stated terms are defined as noted:

State Agency: For purposes of this agreement, the terms State agency, agency, or contractor, refers to the California State agency with which CDSS enters into this agreement.

Confidential Data: Information, the disclosure of which is restricted or prohibited by any provision of law. Some examples of "confidential information" include, but are not limited to, public social services client information described in California Welfare and Institutions Code Section 10850 and "personal information" about individuals as defined in California Civil Code Section 1798.3 of the Information Practices Act (IPA) if the disclosure of the "personal information" is not otherwise allowed by the IPA. Confidential data includes personal identifiers. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data*

Confidential Identifiers: Are specific personal identifiers such as name, social security number, address and date of birth**.**

De-Identification: Removal of personal identifiers**.** Examples of personal identifiers include name, social security numbers, driver's license numbers, and account numbers with access codes. Personal information does not include publicly available information that is lawfully made available to the general public. (See definitions for confidential data and confidential/ personal identifiers.)

Information Assets: Information assets include anything used to process or store information, including (but not limited to) records, files, networks, and databases; information technology facilities, equipment (including personal computer systems), and software (owned or leased).

Information Security Incidents: Information Security incidents include, but are not limited to, the following; any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of CDSS information assets.

Risk: The likelihood or probability that a loss of information assets or breach of security will occur.

Signature of Authorized State Official: Authorized signature shall be determined by the state agency. It is recommended that the agency ISO or individual responsible for oversight of the security requirements in the agreement, review and sign the compliance statement.

EXHIBIT D

Dispute Resolution regarding the Health Insurance Portability and Accountability Act (HIPAA) De-identification of Data 45 CFR 164.514(a) and b(1) and b(2)

1. Describe the study or intended use of the data, (authority for data use, purpose, and subject population described in the data elements) that has been de-identified pursuant to HIPAA regulations

2. Describe the de-identification method or procedures engaged in to make the determination the data is properly de-identified

3. Describe the objections to the de-identification method(s) used or an explanation why there is a reasonable basis to believe that the data can be used to identify an individual

4. Response that de-identification meets HIPAA requirements and/or there is no reasonable basis to believe data can be used to identify an individual.

Attach any documents that are relevant to resolving the dispute.