California *Department* of Social Services
California Department of Health Care Services

MEMORANDUM OF UNDERSTANDING
BETWEEN THE CALIFORNIA DEPARTMENT OF SOCIAL SERVICES AND THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES, AS THE COMPACT ADMINISTRATOR AND COMPACT CO-ADMINISTRATOR
AND
THE COUNTY OF SANTA BARBARA

I. Background and Purpose

Pursuant to the authority granted by California Welfare and Institutions Code (WIC) Section 16121.2 and Sections 16170-16175, California is a member of the Interstate Compact on Adoption and Medical Assistance (ICAMA). The California Department of Social Services (CDSS) and the California Department of Health Care Services (DHCS), as the Compact Administrator and Compact Co-Administrator respectively, have entered into a Memorandum of Understanding with the Association of Administrators of the Interstate Compact on Adoption and Medical Assistance (AAICAMA) for the implementation of a cloud based database (hereinafter "AAICAMA database"). The AAICAMA database replaces the paper ICAMA 700 form and is used to open Medicaid cases between states for adopted special needs children. AAICAMA has contracted with Blue Iron Network for services supporting the AAICAMA database.

The purpose of this Memorandum of Understanding (hereinafter the "MOU") is to outline the terms and conditions for CDSS and DHCS to work with Counties of California for the implementation and utilization of the AAICAMA database to permit the transfer of information between states for establishment of medical benefits for children with adoption assistance agreements and for the provision of training and technical assistance for database users.

This MOU is entered into by the CDSS and DHCS, and the County named above (County), for the purpose of authorizing County access to the AAICAMA database. This MOU authorizes County to facilitate the transfer of information between states for establishment of medical benefits for children with adoption assistance agreements through the AAICAMA database. County agrees to comply with the obligations of this MOU as a condition of access to the AAICAMA database.

II. CDSS and DHCS Responsibilities and Rights

A. The CDSS and DHCS agree to provide the following services:

1. CDSS will coordinate training for all operations and California ICAMA liaisons;

2. CDSS will identify user roles;

3. CDSS will communicate user access changes to AAICAMA; and

4. CDSS and DHCS will report and respond to any security threat or data breach in accordance with approved policies.

B. The CDSS and DHCS have the right as the pass-through entities to inspect, review, or otherwise monitor all activities, procedures, records, reports or forms related to the County's access of the AAICAMA database in order to ensure compliance with this MOU.

III. County Responsibilities

A. County shall maintain any and all information/data provided by the AAICAMA database in strict confidence, and will not reproduce, disclose, or make accessible in whole or in part, in any manner whatsoever, to any third party, unless mandated by law.

B. County represents and warrants it is administering a government funded benefit or program, has been granted the legal authority to view the information/data by the consumer or by operation of law, and shall only request the information/data in compliance with state and federal laws.

C. County certifies that it will order data from the AAICAMA database only when it intends to use the data in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and all state law HIPAA counterparts and the Medi-Cal confidentiality requirements under Welfare and Institutions Code Section 14100.2, as though the data is being used in connection with a determination of the consumer's eligibility for benefits granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status, and for no other purpose. Attachment 1, Exhibit A is the required HIPAA Business Associate Addendum to be executed by County and DHCS.

D. County certifies it will establish safeguards to ensure only Authorized Users can have access to the AAICAMA database. "Authorized User" is defined as a County employee authorized to order or access the AAICAMA database in relation to the performance of their official duties. County shall provide CDSS with a signed ICAMA Database User Policy for each Authorized User.

E. County shall take all necessary measures to prevent unauthorized ordering of or access to the AAICAMA database by any person other than the Authorized User for permissible purposes. County agrees to monitor County employees' access of the AAICAMA database to prohibit employees from using their positions for a purpose that is or gives the appearance of being motivated by a desire for private gain for themselves or others.

F. County agrees to indemnify, defend, and save harmless CDSS, DHCS and Blue Iron, and their respective directors, officers, managers, agents, and employees from any and all claims, actions, demands, damages, liabilities, obligations, losses, settlements, judgments, fines, penalties, sanctions, charges, costs and expenses, arising out of, relating to, or in connection with County's use of the AAICAMA database and/or the unauthorized disclosure or dissemination of consumer-recipient information/data by County employees in the performance of this Agreement. County does not assume the risk on behalf of, or agree to indemnify, any other county.

G. County acknowledges that neither Blue Iron nor its officers, agents or employees will be liable for loss of profits or for indirect, special, incidental or consequential damages arising out of or related to the provision of verifications of employment and/or income, even if that party has been advised of the possibility of such damages. In no event shall damages of any kind payable by Blue Iron exceed the sum paid by CDSS or DHCS for the service which causes County's claim. This provision shall survive any termination or expiration of this MOU.

H. County shall notify CDSS to add or delete a User ID.

I. County hereby certifies it will employ all necessary measures to maintain data security and confidentiality when sending, transferring, or otherwise disposing of any consumer report information. In addition to any requirements of this MOU, County agrees to comply with the HIPAA data security and confidentiality requirements in Attachment 1, Exhibit A and the data security and confidentiality provisions of Attachment 2, Exhibit B – CDSS Confidentiality and Security Requirements.

J. County shall ensure that all County employees comply with WIC sections 10850 and 14100.2 to protect any confidential information it may receive and possess from the AAICAMA database

from unauthorized use, access, or disclosure.

K. Unauthorized use, access, or disclosure of confidential information is considered a breach of security. County shall immediately notify CDSS and DHCS of any and all suspected, attempted, or confirmed breach of security by contacting the CDSS Information Security Officer, Lloyd Indig at (916) 651-5558 and iso@dss.ca.gov and the DHCS Information Security Officer, Steve Moore at (916) 440-7191 and iso@dhcs.ca.gov.

L. The use of the AAICAMA database includes information that is protected by the HIPAA and the Medi-Cal confidentiality and privacy rules and may subject an unauthorized user to possible civil and criminal liability, punishable by fines and imprisonment.

M. Without limitation as to any other applicable rights or remedies, in the event of a breach of security caused by County employee(s), through the use of the information/data provided by Blue Iron, County is responsible for any and all breach notifications to the consumer, any legally required identity theft and/or credit monitoring services, along with associated costs.

N. County may not assign or delegate any of its rights or duties under this MOU.

O. County acknowledges that its access to the AAICAMA database is subject to audit by Blue Iron. County agrees to cooperate with CDSS, DHCS, and Blue Iron in responding to any such audit.

IV. Effective Date and Term

This MOU is effective on the date that it is signed by all parties. The initial term of this MOU shall be for a period of one year commencing on the effective date. Upon the expiration of the initial term, this MOU shall automatically renew for successive one-year terms unless terminated by any party as provided in Section VI below.

V. Project Representatives

The primary points of contact for the parties pursuant to this MOU are:

For CDSS:

Steve Shields, Manager
Adoption Services Bureau
Children's Services Operation and Evaluation Branch
Children and Family Services Division
California Department of Social Services
744 P Street, M.S. 8-12-31
Sacramento, CA 95814
Phone: (916) 651-8086
Email: Steve.Shields@dss.ca.gov

For DHCS:

Jeanette M. Barajas, Chief
Access Programs & Policy Branch
Medi-Cal Eligibility Division
Department of Health Care Services
1501 Capitol Avenue
P.O. Box 997417, MS-4607
Sacramento, CA 95899-7417
Phone: (916) 552-9413
Fax: (916) 440-5644
E-mail: Jeanette.Barajas@dhcs.ca.gov

For AAICAMA:

Robin Bockweg, Project Director
Association of Administrators of the Interstate Compact on Adoption and Medical Assistance
1133 Nineteenth Street, NW
Washington, DC 20036
Phone: (202) 682-0100
Email: RBockweg@aphsa.org

For Blue Iron:

Stephen Sarrouf
Blue Iron Network

5811 McFadden Avenue
Huntington Beach, CA 92649
Phone: (855)258-4766
Email: stephen_sarrouf@blueironnetwork.com

VI. General Provisions

A. No condition or provision of this MOU shall be waived or altered except by written amendment signed by a duly authorized representative of CDSS, DHCS, and County.

B. Termination without cause: This MOU may be terminated by any party without cause upon 30 days written notice.

C. Termination with cause: This MOU may be terminated immediately by any party if the terms of this MOU are violated in any manner. However, CDSS, DHCS, or County shall provide written notice to the other parties of such termination for cause of this MOU. Blue Iron may immediately suspend and/or terminate County's access to the AAICAMA database if Blue Iron reasonably believes County has violated the HIPAA, any of the state law counterparts to the HIPAA, the Medicaid and Medi-Cal confidentiality laws, or any other applicable law or regulation.

D. Other grounds for Termination: In the event that any of the companion agreements, contracts or MOUs discussed in Section I - Background and Purpose terminate or expire, this MOU may be terminated on the effective date of the termination of that companion agreement, contract or MOU even if such termination will occur with less than 30 days written notice.

CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

By: _____

Name: Deborah Pearce

Title: Chief, Contracts and Purchasing Bureau

Date: _____

CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

By: _____

Name: _____

Title: _____

Date: _____

COUNTY OF SANTA BARBARA

By: _____

Name: _____

Title: _____

Date: _____

Attachment 1 – Exhibit A - HIPAA Business Associate Addendum
Attachment 2 – Exhibit B - Confidentiality and Security Requirements

Exhibit A
HIPAA Business Associate Addendum

I. Recitals

A. This **BUSINESS ASSOCIATE ADDENDUM** (this "Addendum") is made by and between The California Department of Health Care Services ("Covered Entity" or "DHCS") and COUNTY of Santa Barbara ("Business Associate" or "Contractor"). Covered Entity and Business Associate are parties to a Memorandum of Understanding for Business Associate's use of the AAICAMA cloud based database, ("Services Agreement"), which 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. DHCS wishes to disclose to Business Associate certain information pursuant to the terms of the Services 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 the Services Agreement Business Associate may create, receive, maintain, transmit, use or disclose PHI and PI on DHCS' behalf. DHCS and Business Associate are each a party to this Addendum 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 the Services 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 generally have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule, but as used in this Addendum shall mean COUNTY of Santa Barbara.

C. Covered Entity shall generally have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule, but as used in this Addendum shall mean the California Department of Health Care Services.

Exhibit A
HIPAA Business Associate Addendum

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.

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, but for purposes of this Addendum is limited to information received by Business Associate from Covered Entity, or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

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 or PHI means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103, but for purposes of this Addendum is limited to information received by Business Associate from Covered Entity, or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

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.

Exhibit A
HIPAA Business Associate Addendum

III. Terms of Agreement

A. Permitted Uses and Disclosures of PHI by Business Associate

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

   c. ***Report Violations of the Law.*** Business Associate may use PHI to report violations of law to appropriate State or Federal Authorities, consistent with 45 C.F.R 164.502(j).

   d. ***De-Identification***. Business Associate may de-identify PHI, but must do so in accordance with 45 CFR section 164.514(b), and Business Associate may use such de-identified information solely for the benefit of Covered Entity for any purpose related to the services being provided to Covered Entity under the Services Agreement**.**

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).

Exhibit A
HIPAA Business Associate Addendum

C. Responsibilities of Business Associate

Business Associate agrees:

1. ***Nondisclosure***. Not to use or disclose Protected Health Information other than as permitted or required by this Addendum 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 ePHI, 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 Addendum. 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. 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 in violation of the requirements of this Addendum. As all Business Associate subcontractor agreements include mitigation clauses, Business Associate acknowledges its obligation and responsibility for enforcement of such separate mitigation obligations.

Exhibit A
HIPAA Business Associate 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 under HIPAA 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 non-employee 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 sub award 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. Business Associate will incorporate those portions of this Addendum that it determines are applicable into any subcontract and subaward with agents, subcontractors, and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate,

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 the extent that the Services Agreement requires Business Associate to maintain PHI in a Designated Record Set under its custody and control, provide access as DHCS may reasonably require, and in the time and manner designated by DHCS in writing (upon reasonable notice and during Business Associate's normal business hours, if applicable) to PHI in such 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 written request by producing the records or verifying that there are none.

2. If Business Associate maintains, pursuant to the Services Agreement, an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic

Exhibit A
HIPAA Business Associate Addendum

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).

G. ***Amendment of PHI.*** To the extent that the Services Agreement requires Business Associate to maintain PHI in a Designated Record Set under its custody and control, make any amendment(s) to PHI that DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner reasonably 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. Any rights of DHCS to access Business Associate's internal practices, books and records is governed by the audit rights set forth in Section V hereof.

I. ***Documentation of Disclosures.*** To the extent no exception exists under 45 CFR section 164.528, 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).

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 **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 involving PHI or PI, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Addendum. A Breach shall be treated as discovered by Business Associate as of the first business 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. 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 selected "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 involving PHI, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Addendum, Business Associate shall take:

Exhibit A
HIPAA Business Associate Addendum

a. Prompt corrective action to mitigate any risks or damages involved with the Breach known to Business Associate and to protect the operating environment; and

b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations, including the provision of any required notices as set forth in Section (III)(J)(4) below.

2. ***Investigation and Investigation Report.*** To immediately investigate such security incident involving PHI, Breach, or unauthorized access, use or disclosure of PHI or PI in violation of this Addendum. Within five (5) days of the discovery, Business Associate shall submit a "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 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

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, determine whether it is reportable to the appropriate entities, and if individual notifications are required. Business Associate will provide any corrective action plan to DHCS for review. .

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 as a result of the Breach or unauthorized use or disclosure when notification is required under state or federal law, and Business Associate shall pay the cost of such notifications, as well as up to 12 months of any credit monitoring reasonably offered as a result of the Breach. The notifications shall comply with the requirements set for 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 less 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, which approval shall not be unreasonably delayed or withheld.

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

Exhibit A
HIPAA Business Associate Addendum

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

DHCS Program Contract Manager	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Memorandum of Understanding for Program Contract Manager (Project Representative) 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 Services 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 Services Agreement if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or

2. Immediately terminate the Services 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 non-employee agents, subcontractors and vendors are in compliance with their obligations as required by their respective written agreements.

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.

Exhibit A
HIPAA Business Associate Addendum

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.

C. ***Notification of Restrictions***. Timely notify the Business Associate in writing 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 (limited solely to those systems that contain PHI), books and records of Business Associate to monitor compliance with the Services Agreement and this Addendum. Business Associate may require DHCS, or any third party acting on behalf of DHCS, to sign a confidentiality agreement acceptable to Business Associate prior to providing access to Business Associate's books, records, and systems pursuant to this Section. 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).

Exhibit A
HIPAA Business Associate Addendum

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 Services Agreement 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 a reasonable time as 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.

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. Either party may terminate the Services Agreement if the other party is found guilty of a criminal violation of HIPAA. DHCS may terminate the Services 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 Addendum 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 to the extent that amendments are necessary in order for this Addendum to remain compliant with applicable law. Upon DHCS' request, Business Associate agrees to

Exhibit A
HIPAA Business Associate Addendum

promptly enter into negotiations with DHCS concerning such an amendment to this Addendum. DHCS may terminate this Agreement upon thirty (30) days written notice in the event:

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

2. Business Associate does not enter into the required amendment that is necessary to maintain compliance with applicable law.

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 mutually convenient times and places 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.

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 permitted 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 the required provisions of 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 the required provisions of 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.

I. **Entire Agreement.** This Addendum and the Services Agreement shall constitute the entire agreement of the parties hereto with respect to the subject matter hereof and supersede all prior agreements, understandings and representations, whether oral or written, relating to such subject matter.

J. **Severability.** If any provision of this Addendum is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Addendum shall otherwise remain in full force and effect and enforceable.

K. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to its conflicts of laws principles, to the extent not preempted by HIPAA or other applicable federal law.

Exhibit A
HIPAA Business Associate Addendum

BUSINESS ASSOCIATE:
COUNTY OF SANTA BARBARA

By: _____

Name: _____

Title: _____

Date: _____

COVERED ENTITY:
DHCS

By: _____

Name: _____

Title: _____

Date: _____

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. ***Confidentially Statement***. All employees execute a Non-Disclosure Agreement at the time of hire.

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.

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.

Exhibit A
HIPAA Business Associate Addendum

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.

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.

Exhibit A
HIPAA Business Associate Addendum

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

The section is applicably only if, and when, Contractor converts DHCS PHI or PI into paper form for use and handling in a manner consistent with the terms of provisions of this Addendum.

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.

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.

Exhibit B
The California Department of Social Services
Confidentiality and Information Security Requirements – Contractor/Entity

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as "this Exhibit") sets forth the information security and privacy requirements Contractor/Entity (hereinafter referred to as "Contractor") is obligated to follow with respect to all confidential and sensitive information (as defined herein) disclosed to or collected by Contractor, pursuant to Contractor's Agreement (the "Agreement") with the California Department of Social Services (hereinafter "CDSS") in which this Exhibit is incorporated. The CDSS and Contractor desire to protect the privacy and provide for the security of CDSS Confidential, Sensitive, and/or Personal (CSP) Information in (hereinafter referred to as "CDSS CSP") compliance with state and federal statutes, rules and regulations.

I. Order of Precedence. With respect to information security and privacy requirements for all CDSS CSP, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between Contractor and CDSS and shall prevail over any such conflicting terms or conditions.

II. Effect on lower tier transactions. The terms of this Exhibit shall apply to all lower tier transactions (e.g. agreements, sub-agreements, contracts, subcontracts, and sub-awards, etc.) regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each lower tier transaction to its agents, contractors, subcontractors, or independent consultants, etc.

III. Confidentiality of Information.

a. DEFINITIONS. The following definitions relate to CDSS Confidential, Sensitive, and/or Personal Information.

i. "Confidential Information" is information maintained by the CDSS that is exempt from disclosure under the provisions of the California Public Records Act (Government Codes Sections 6250-6265) or has restrictions on disclosure in accordance with other applicable state or federal laws.

ii. "Sensitive Information" is information maintained by the CDSS, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information is information in which the disclosure would jeopardize the integrity of the CDSS (i.e., CDSS' fiscal resources and operations).

iii. "Personal Information" is information, in any medium (paper, electronic, or oral) that identifies or describes an individual (i.e., name, social security number, driver's license, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information (PHI), etc.) and must be protected from inappropriate access, use or disclosure and must be made accessible to information subjects upon request. It can also be information in the possession of the Department in which the disclosure is limited by law or contractual Agreement (i.e., proprietary information, etc.).

iv. "Breach" is

1. the unauthorized acquisition, access, use, or disclosure of CDSS CSP in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

v. "Security Incident" is

1. an attempted breach;
2. the attempted or successful unauthorized access or disclosure, modification or destruction of CDSS CSP, in violation of any state or federal law or in a manner not permitted under the Agreement between Contractor and CDSS, including this Exhibit; or
3. the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDSS CSP.

b. CDSS CSP by the CDSS which may become available to the Contractor as a result of the implementation of the Agreement shall be protected by the Contractor from unauthorized access, use, and disclosure as described in this Exhibit.

c. Contractor is notified that unauthorized disclosure of CDSS CSP may be subject to civil and/or criminal penalties under state and federal law, including but not limited to:

- California Welfare and Institutions Code section 10850
- Information Practices Act – California Civil Code section 1798 et seq.
- Public Records Act – California Government Code section 6250 et seq.
- California Penal Code Section 502, 11140-11144, 13301-13303
- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") – 45 CFR Parts 160 and 164
- Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50

d. EXCLUSIONS. "Confidential Information", "Sensitive Information", and "Personal Information" (CDSS CSP) does not include information that

i. is or becomes generally known or available to the public other than because of a breach by Contractor of these confidentiality provisions;

ii. already known to Contractor before receipt from CDSS without an obligation of confidentiality owed to CDSS;

iii. provided to Contractor from a third party except where Contractor knows, or reasonably should know, that the disclosure constitutes a breach of confidentiality or a wrongful or tortious act; or

iv. independently developed by Contractor without reference to the CDSS CSP.

IV. Contractor Responsibilities.

a. Training. The Contractor shall instruct all employees, agents, and subcontractors with access to the CDSS CSP regarding:

i. The confidential nature of the information;

ii. The civil and criminal sanctions against unauthorized access, use, or disclosure found in the California Civil Code Section 1798.55, Penal Code Section 502 and other state and federal laws;

iii. CDSS procedures for reporting actual or suspected information security incidents in Paragraph V – Information Security Incidents and/or Breaches; and

iv. That unauthorized access, use, or disclosure of CDSS CSP is grounds for immediate termination of this Agreement with CDSS and the Contractor and may be subject to penalties, both civil and criminal.

b. Use Restrictions. The Contractor shall ensure that their employees, agents, contractors, subcontractors, and independent consultants will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement.

c. Disclosure. The Contractor shall not disclose any individually identifiable CDSS CSP to any person other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement. Contractor is permitted to disclose individually identifiable CDSS CSP with the consent of the individual to its service providers, its vendors, and its partners for the purposes of Contractor providing services to CDSS or otherwise to meet Contractor's obligations under the Agreement. For CDSS CSP, Contractor must provide CDSS Program Manager and CDSS Information Security Office with a list of Contractor authorized service providers and ensure they are bound by obligations sufficient to protect CDSS CSP in accordance with this Agreement.

d. Subpoena. If Contractor receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CDSS CSP, Contractor will immediately notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer. In no event should notification to CDSS occur more than twenty-four (24) hours after knowingly receiving such request.

e. Information Security Officer. The Contractor shall designate an Information Security Officer to oversee its compliance with this Exhibit and to communicate with CDSS on matters concerning this Exhibit.

f. Requests for CDSS CSP by Third Parties. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer all requests for disclosure of any CDSS CSP requested by third parties to the Agreement between Contractor and CDSS (except from an Individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

g. Documentation of Disclosures for Requests for Accounting. Contractor shall maintain an accurate accounting of all requests for disclosure of CDSS CSP Information and the information necessary to respond to a request for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

h. Return or Destruction of CDSS CSP on Expiration or Termination. Upon expiration or termination of the Agreement between Contractor and CDSS for any reason, Contractor shall return or destroy the CDSS CSP. If return or destruction is not feasible, Contractor shall provide a written explanation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information in this Agreement. CDSS, in its sole discretion, will make a determination of the acceptability of the explanation and, if retention is permitted, shall inform Contractor in writing of any additional terms and conditions applicable to the retention of the CDSS CSP.

i. Retention Required by Law. If required by state or federal law, Contractor may retain, after expiration or termination, CDSS CSP for the time specified as necessary to comply with the law.

j. Obligations Continue Until Return or Destruction. Contractor's obligations regarding the confidentiality of CDSS CSP set forth in this Agreement, including but not limited to obligations related to responding to Public Records Act requests and subpoenas shall continue until Contractor returns or destroys the CDSS CSP or returns the CDSS CSP to CDSS; provided however, that on expiration or termination of the Agreement between Contractor and CDSS, Contractor shall not further use or disclose the CDSS CSP except as required by state or federal law.

k. Notification of Election to Destroy CDSS CSP. If Contractor elects to destroy the CDSS CSP, Contractor shall certify in writing, to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information, that the CDSS CSP has been destroyed.

l. Background Check. Before a member of the Contractor's workforce may access CDSS CSP, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to the State's information technology systems and the data contained therein. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following Agreement termination.

m. Confidentiality Safeguards. The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the CDSS CSP that it creates, receives, maintains, uses, or transmits pursuant to the Agreement. Contractor 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 Contractor's operations and the nature and scope of its activities, including at a minimum the following safeguards:

i. General Security Controls

1. ***User Confidentiality Statement.*** All persons with access to CDSS CSP must sign the CDSS User Confidentiality Agreement (Exhibit E, Attachment 2). The statement must be signed prior to access to CDSS CSP. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDSS inspection for a period of three (3) years following contract termination.
2. **Workstation/Laptop Encryption.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDSS Information Security Office.
3. **Data Encryption.** Any CDSS CSP shall be encrypted at rest when stored on network file shares or document repositories.
4. **Server Security.** Servers containing unencrypted CDSS CSP must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
5. **Minimum Necessary.** Only the minimum necessary amount of the CDSS CSP required to perform necessary business functions may be copied, downloaded, or exported.
6. **Removable Media Devices.** All electronic files that contain the CDSS CSP must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart phone, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.

7. **Antivirus Software.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

8. **Patch Management.** Contractor must submit a documented patch management system, to be approved by the CDSS Information Security Office, in place to install security patches in a timely manner on all Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP as appropriate based on Contractor's risk assessment of such patches, the technical requirements of Contractor's systems, and vendor's written recommendations. In lieu of an approved patch management system, all applicable patches must be installed within thirty (30) days of vendor release or patch installation occurs within the CDSS approved timeframes by the next scheduled change release, or accept risk with an approved risk analysis by the Contractor.

9. **User IDs and Password Controls.** All users must be issued a unique user name for accessing CDSS CSP which meets or exceeds CDSS current Password policy. (Contact CDSS Information Security and Privacy Officer for current policy.)

10. **Data Destruction.** Upon termination of the Agreement, all CDSS CSP must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDSS Information Security Office.

ii. System Security Controls

1. **System Timeout.** The system providing access to the CDSS CSP must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

2. **Warning Banners.** All systems containing CDSS CSP must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

3. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDSS CSP, or which alters CDSS CSP. 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 CDSS CSP is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence.

4. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

5. **Transmission Encryption.** All data transmissions of CDSS CSP outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDSS CSP can be encrypted. This requirement pertains to any type of CDSS CSP in motion such as website access, file transfer, and E-Mail.

6. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting CDSS CSP that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

iii. Audit Controls

1. **System Security Review.** All systems processing and/or storing CDSS CSP 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 shall include vulnerability scanning tools.
2. **Log Reviews.** All systems processing and/or storing CDSS CSP must have a routine procedure in place to review system logs for unauthorized access.
3. **Change Control.** All systems processing and/or storing CDSS CSP 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

1. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDSS CSP 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 twenty-four (24) hours.
2. **Data Backup Plan.** Contractor must have established documented procedures to backup CDSS CSP to maintain retrievable exact copies of CDSS CSP. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDSS CSP should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDSS data.

v. Paper Document Controls

1. **Supervision of Information**. CDSS CSP 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 may be observed by an individual not authorized to access the information. CDSS CSP 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.
2. **Escorting Visitors**. Visitors to areas where the CDSS CSP are contained shall be escorted and CDSS CSP shall be kept out of sight while visitors are in the area.
3. **Confidential Destruction**. CDSS CSP must be disposed of through confidential means, such as cross cut shredding and/or pulverizing.
4. **Removal of Information**. CDSS CSP must not be removed from the premises of the Contractor except for identified routine business purposes or with express written permission of CDSS.
5. **Faxing**. CDSS CSP that must be transmitted by fax shall require that the Contractor confirms the recipient fax number before sending, takes

precautions to ensure that the fax was appropriately received, maintains procedures to notify recipients if the Contractor's fax number changes, and maintains fax machines in a secure area**.**

6. **Mailing**. Paper copies of CDSS CSP shall be mailed using a secure, bonded mail service, such as Federal Express, UPS, or by registered U.S. Postal Service (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.

V. Information Security Incidents and/or Breaches

a. Incidents and/or Breaches Response Responsibility. The Contractor shall be responsible for facilitating the Incident and/or Breach response process as described in California Civil Code 1798.29(e), California Civil Code 1798.82(f), and SAM 5340, Incident Management.

b. Discovery and Notification of Incidents and/or Breaches. The Contractor shall notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within one working day by telephone call and email upon the discovery of the Incident and/or Breach affecting the security of CDSS CSP if the CDSS CSP was, or is reasonably believed to have been, acquired by an unauthorized person, or there is an intrusion, potential loss, actual loss, or unauthorized use or disclosure of the CDSS CSP is in violation of this Agreement, this provision, or applicable law. The Contractor shall take:

i. Prompt corrective action to mitigate the risks or damages involved with the Incident and/or Breach and to protect the operating environment; and

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

c. Isolation of System or Device. A system or device, containing CDSS CSP, compromised by an Incident and/or Breach involving an exploitation of a technical vulnerability, shall be promptly disconnected from Contractor's production environment with access to only individuals who are participating in the investigation, mitigation, and remediation of the Incident and/or Breach. Such system or device shall remain disconnected from the production environment until the risk from the exploited vulnerability has been adequately mitigated. CDSS must be contacted prior to placing the previously compromised system or device, containing CDSS CSP, back in the production environment. The affected system or device, containing CDSS CSP, shall not be returned to operation in the production environment until the CDSS Information Security and Privacy Officer gives its approval.

d. Investigation of Incidents and/or Breaches. The Contractor shall promptly investigate such Incidents and/or Breaches.

e. Updates on Investigation. The Contractor shall provide regular (at least once a week) email updates on the progress of the Incident and/or Breach investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer until they are no longer needed, as mutually agreed upon between the Contractor and the CDSS Information Security and Privacy Officer.

f. Written Report. The Contractor shall provide a written report of the investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within ten (10) working days of the discovery of the Incident and/or Breach. To the extent Contractor has such information, the report shall include but not be limited to the following:

i. Contractor point of contact information;

ii. Description of what happened, including the date of the Incident and/or Breach and the date of the discovery of the Incident and/or Breach, if known;

iii. Description of the types of CDSS CSP that were involved and the extent of the information involved in the Incident and/or Breach;

iv. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CDSS CSP;

v. A description of where the CDSS CSP is believed to have been improperly transmitted, sent, or utilized;

vi. A description of the probable causes of the improper use or disclosure;

vii. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered; and

viii. Full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Incident and/or Breach.

g. Notification of Individuals. The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under applicable state or federal law as reasonably determined by CDSS. Contractor shall be responsible for the notifications, as well as any costs associated with the breach. The CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer shall promptly approve the time, manner and content of any such notifications, and such approval shall not be unreasonably withheld.

VI. Contact Information. To direct communications to the above referenced CDSS staff, the Contractor shall initiate contact as indicated herein. CDSS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

CDSS Program Contract Manager	**CDSS Information Security & Privacy Officer**
See the Scope of Work exhibit for Program Contract Manager information	California Department of Social Services Information Security & Privacy Officer 744 P Street, MS 9-9-70 Sacramento, CA 95814 Email: iso@dss.ca.gov Telephone: (916) 651-5558

VII. Audits and Inspections. From time to time, CDSS may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer in writing. The fact that CDSS inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit.

VIII. Amendment. The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CDSS CSP.

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

X. Termination. An information Incident and/or Breach by Contractor, its employees, agents, or subcontractors, as determined by CDSS, may constitute a material breach of the Agreement between Contractor and CDSS and grounds for immediate termination of the Agreement.

CALIFORNIA DEPARTMENT of SOCIAL SERVICES
USER CONFIDENTIALITY AGREEMENT

Information resources maintained by the California Department of Social Services (CDSS) and provided to your entity may be confidential, sensitive, and/or personal. Confidential, Sensitive, and/or Personal (CSP) information is not open to the public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. The CDSS strictly enforces information security. If you violate these provisions, you may be subject to administrative, civil, and/or criminal penalty.

_____ INITIAL I hereby acknowledge that the confidential and/or sensitive records of the CDSS are subject to strict confidentiality requirements imposed by state and federal law include the California Welfare and Institutions Code §10850, Information Practices Act – California Civil Code §1798 et seq., Public Records Act – California Government Code §6250 et seq., California Penal Code §502, 11140-11144, 13301-13303, Health Insurance Portability and Accountability Act of 1996 ("HIPAA") – 45 CFR Parts 160 and 164, and Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50.

_____ INITIAL I acknowledge that my supervisor reviewed with me the confidentiality and security requirements, policies, and administrative processes of my organization, the CDSS, and of the State.

_____ INITIAL I acknowledge that I will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement.

_____ INITIAL I acknowledge that the Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other entity workforce members under Contractor's direct control who intentionally or negligently violate any provisions of this Exhibit.

_____ INITIAL I acknowledge that unauthorized access, use, or disclosure of CDSS CSP is grounds for immediate termination of this Agreement with CDSS and the Contractor and may be subject to penalties, both civil and criminal.

_____ INITIAL I hereby agree to protect the CDSS' information on either paper or electronic form by:

- Only accessing or using the CDSS supplied information as specified in the Agreement for the performance of the specific work I am assigned.
- Never accessing information for curiosity or personal reasons.
- Never showing or discussing CSP information to or with anyone who does not have the need to know.
- Never removing CSP information from the work site without authorization.
- Following encryption requirements for all CSP information in any portable device or media.

"I certify that I have read and initialed the confidentiality statements printed above and will abide by them."

Name (Printed): _____

Signature: _____

Date Signed: _____