SYSTEM DATA AGREEMENT FOR
FREE OR REDUCED-PRICE SCHOOL LUNCH OR BREAKFAST
BETWEEN [BLANK] AND
SAN DIEGO COUNTY HEALTH & HUMAN SERVICES AGENCY FOR
CALWIN DATA EXTRACT OF CONFIDENTIAL FILES

I. Participants

The Health and Human Services Agency (HHSA) and **[BLANK]** are entering into this System Data Agreement (SDA) for CalWIN Data extract of Confidential Files.

II. Administration of SDA

Each party identifies the following individual to serve as the authorized administrative representative for that party. Any party may change its administrative representative by notifying the other party in writing of such change. Any such change will become effective upon the receipt of such notice by the other party to this SDA. Notice of the authorized representative should be sent to each party as follows:

County of San Diego Health & Human Services Agency 1255 Imperial Ave, Suite 446 San Diego, CA 92101 (619) 338-2313 Attn: Charline Khoury, Chief, Eligibility Operations	**[BLANK]** **NAME** **ADDRESS** **PHONE NUMBER** **EMAIL ADDRESS** **CONTACT PERSON** **CONTACT PERSON EMAIL ADDRESS**

III. Purpose

The purpose of this agreement is for **[BLANK]** to provide HHSA a listing of the children currently enrolled at **[BLANK]** and to set the parameters and responsibilities for this agreement. This SDA is also to meet the provisions of the U.S. Federal Child Nutrition and WIC Reauthorization Act of 1989, §202(b) (1). This act allows a designated school food authority to certify a student as eligible for a free or reduced-price school lunch or breakfast, without further application, by directly communicating with the appropriate local agency to obtain documentation of student's status as a member of a CalFresh household.

IV. Requirements for Match

A. **[BLANK]** Requirements: **[BLANK]** staff provide school records of children enrolled in the **[BLANK]**. Those children who are in households that receive CalFresh will be so indicated by the match to confirm eligibility for a free or reduced school lunch/breakfast.

B. HHSA Requirements: HHSA will provide **[BLANK]** a match from CalWIN of

children that are eligible to receive CalFresh in the report month.

V. Indemnity

County of San Diego shall not be liable for, and **[BLANK]** shall defend and indemnify County and the employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs (hereinafter collectively referred to as "Claims"), related to this SDA and arising either directly or indirectly from any act, error, omission or negligence of **[BLANK]** or its contractors, licensees, agents, servants or employees, including, without limitation, Claims caused by the concurrent negligent act, error or omission, whether active or passive, of County Parties. **[BLANK]** shall have no obligation, however, to defend or indemnify County Parties from a Claim if it is determined by a court of competent jurisdiction that such Claim was caused by the sole negligence or willful misconduct of County Parties.

VI. Insurance (See Exhibit A)

Prior to execution of this SDA, **[BLANK]** must obtain at its own cost and expense, and keep in force and effect during the term of this agreement including all extensions, the insurance specified in Exhibit "A," "Insurance Requirements," attached hereto.

VII. Conformance With Rules And Regulations

[BLANK] shall be in conformity with all applicable federal, State, County, and local laws, rules, and regulations, current and hereinafter enacted, including facility and professional licensing and/or certification laws and keep in effect any and all licenses, permits, notices and certificates as are required. **[BLANK]** shall further comply with all laws applicable to wages and hours of employment, occupational safety, and to fire safety, health and sanitation.

VIII. Permits and Licenses

[BLANK] certifies that it possesses and shall continue to maintain or shall cause to be obtained and maintained, at no cost to the County, all approvals, permissions, permits, licenses, and other forms of documentation required for it and its employees to comply with all existing foreign or domestic statutes, ordinances, and regulations, or other laws, that may be applicable to performance of services hereunder. The County reserves the right to reasonably request and review all such applications, permits, and licenses prior to the commencement of any services hereunder.

IX. Specific Warranty of Security and Privacy

[BLANK] warrants that the application software provides security and privacy for the system and its data (where "security" is defined as protection of software and data from natural or human-caused hazards and unauthorized access and manipulation, and "privacy" is defined as protection of personal data from

unauthorized access or disclosure), and contains mechanisms to assure integrity of the County's data against destruction, loss or unauthorized alteration. The County hereby acknowledges that fundamental security, privacy and integrity controls are provided by the application software, while differentiating operational mechanisms for protecting data integrity, such as regular data backups performed by its personnel, from these internal controls. **[BLANK]** warrants only that data privacy provided by the software performs as described in the specifications. Notwithstanding the foregoing, **[BLANK]** cannot warrant that another party's backup software will perform properly.

X. Protection of County Confidential Information and Data System

Subject to the disclosure requirements of the Public Records Act, California Government Code Section 6250 – 6268, all reports, information, data, statistics, forms, procedures, systems, studies and any other communication or information given to or prepared or assembled by **[BLANK]** under this agreement, shall be kept confidential, shall not be made available to any individual or organization by **[BLANK]** without the prior written approval of County.

XI. Systems and Network Security

At all times during the term of this Agreement, **[BLANK]** shall provide all services, and use all resources related thereto, in a secure manner and in accordance with the County's security requirements, including the prevention and detection of fraud, abuse, or other inappropriate use or access of systems, networks and/or data by all appropriate means, including network management and maintenance applications and tools, and the use of appropriate encryption technologies. In connection therewith, (i) any attempts by **[BLANK]** personnel to circumvent network security measures or to access or use resources that are not specifically authorized for the **[BLANK]** use in performing under this agreement, and (ii) access to County computer resources or data by unauthorized persons via the **[BLANK]** access User ID's, will constitute misuse of the County's computer and/or data resources. In no event shall **[BLANK]** actions or inaction result in any situation that is less secure than the security **[BLANK]** then provides for its own systems and data. In addition, all **[BLANK]** personnel (including personnel of any sub-contractors) shall be subject to and shall at all times conform to the County's laws, rules, and requirements for the protection of premises, materials, equipment, and personnel, as they may be disclosed to **[BLANK]** in writing. Any violations or disregard of these rules shall be cause for denial of access by such personnel to the County's property, systems, networks and/or data.

XII. Access to County Information

As used herein, the term "County Data" shall mean, in or on any media or form of any kind: (i) all data and summarized data related to the County, its citizens, or the **[BLANK]** services that is in the possession of the County and all data concerning or indexing such data (regardless of whether or not owned by the County, generated or compiled by the County, or provided by its citizens), including data that is in the County's databases or otherwise in the

County's possession at any time; and (ii) all other County records, data, files, input materials, reports, forms, and other such items that may be received, computed, developed, used, or stored by **[BLANK]**, or by any of its sub-contractors, in the performance of **[BLANK]** duties under this Agreement.

XIII. Confidentiality

The use or disclosure of information concerning HHSA applicants and recipients will be limited to use by designated **[BLANK]** staff for the items listed below. Information will not be released to any other agencies except as specified in Welfare & Institutions Code 10850, 10850.2, and 14100.2 that describes the use of confidential records. HHSA records fall within the description of confidential records. **[BLANK]** recognizes that unauthorized release of confidential information may make the individual guilty of a misdemeanor under Welfare & Institutions Code 10850 or 14100.2. It may lead to criminal or civil liability for the individual. The Welfare & Institutions Codes stated above restrict the type and amount of information that may be released. Written consent of the applicant or recipient will be required in order to release information specified under W & I Code 10850.2. It further states that "...written authorization shall be dated and signed by each recipient and shall expire one year from the date of execution." Under W & I Code 10850, 10850.2, and 14100.2 confidential records used by **[BLANK]** staff will be for:

1. Utilize information provided by HHSA from CalWIN to identify children who are in households that receive CalFresh to confirm eligibility for a free or reduced-price school lunch/breakfast.

The participants understand that in questionable situations, the **[BLANK]** staff will seek HHSA agreement prior to releasing any information and that this request will be in written form.

A. **[BLANK]** will provide HHSA a list of employees designated to access CalWIN data specified in lll B. above.

B. **[BLANK]** will maintain a physically secure storage place for all written/electronic formats of data of information gained from HHSA to prevent access by unauthorized persons.

C. **[BLANK]** acknowledges that clearances made through the match shall be only for the administration of information that is necessary to determine eligibility to identify children who are in households that receive CalFresh to confirm eligibility for a free or reduced-price school lunch/breakfast.

D. **[BLANK]** agrees that designated employees will not access their own case assistance data or those of any friend, relative, business relation, personal acquaintance, they may know.

E. In the event that any unauthorized access to or use of confidential data by

any **[BLANK]** employee, **[BLANK]** shall take disciplinary action against the employee, up to and including termination. **[BLANK]** shall notify HHSA when an employee is subject to such disciplinary action.

F. **[BLANK]** agrees that all individually identifiable information furnished by or obtained through the match will be destroyed by shredding or a similar method of destruction once the use for the information has ended.

G. **[BLANK]** agrees to allow the HHSA signatory or authorized representative, as the operating agency for CalWIN, to make on-site inspections to ensure that the terms of this agreement are being met.

H. **[BLANK]** agrees not to release confidential information, which includes individual identifying information such as address, name, etc., to outside agencies or persons that do not fall under Welfare and Institutions Codes 10850 or 14100.2. This information may be released under W & I Code 10850.2 if a properly executed written release of information is obtained by HHSA or **[BLANK].** Any written releases obtained by **[BLANK]** must be maintained in a file for audit purposes.

I. **[BLANK]** agrees to submit a Summary of Policy form for each newly designated staff member who will access and use the information, other than for statistical purposes as allowed under W & I Code 10850, 10850.2, and 14100.2. Copies of each statement must be received by HHSA three (3) days before the designated staff member accesses the information. The copies will be retained by HHSA as part of this agreement.

J. **[BLANK]** agrees to provide updates to HHSA within ten (10) workdays for any designated staff for whom access is being deleted or work location is being changed.

Strict adherence to the criteria stated in items A through J must be followed. Confidential client information may only be accessed by designated staff when the applicable conditions stated in items A through J have been met.

XIV. Organization

The duties to administer, supervise, and monitor the administration and determination for **[BLANK]** under these agreements belongs solely to the **[BLANK]**. The duties to administer, supervise, and monitor CalWIN data access and security belongs solely to the HHSA. As part of this agreement, **[BLANK]** and HHSA agree to cooperate, within regulatory authority, so that the **[BLANK]** may locate or apprehension the recipient is within such official duties and HHSA may carry out regulatory and security responsibilities for CalWIN matches.

XV. Contractor's Confidential Records

Any reports, information, data, statistics, forms, procedures, systems, studies and

any other communication or information given to or prepared or assembled by San Diego County under this agreement, will be kept confidential, and shall not be made available to any individual or organization by County without the prior written approval of **[BLANK]**.

XVI. Standards

Both HHSA and **[BLANK]** shall maintain an organizational structure and sufficient staff, within any budgetary constraints, to efficiently and effectively administer and supervise the functions and responsibilities set out in this agreement.

XVII. HHSA Responsibilities and Duties

HHSA will ensure that all approved processes and instructions are followed to ensure the requested information is provided to authorize **[BLANK]** staff.

XVIII. Governing Law

This SDA shall be governed, interpreted, construed and enforced in accordance with the laws of the State of California.

XIX. Third Party Beneficiaries Excluded

This SDA is intended solely for the benefit of the County and **[BLANK]**. Any benefit to any third party is incidental and does not confer on any third party to this SDA any rights whatsoever regarding the performance of this SDA. Any attempt to enforce provisions of this SDA by third parties is specifically prohibited.

XX. Amendments to SDA

Any party may propose amendments to this SDA by providing written notice of such amendments to the other party. This SDA may only be amended by a written amendment signed by both parties.

XXI. Severability

If any terms provisions of this SDA or the application thereof to any person or circumstance shall, to any extent, be held invalid or unenforceable, the remainder of this SDA, or the application of such term and provision to persons or circumstances other than those as to which it is held invalid or unenforceable, shall not be affected thereby and every other term and provision of this SDA shall be valid and enforceable, shall not be affected thereby and every other term and provision of this SDA shall be valid and enforced to the maximum extent permitted by law.

XXII. Full Agreement

This SDA represents the full and entire agreement between the parties and supersedes any prior written or oral agreements that may have existed.

XXIII. Scope of SDA

This SDA only applies to the program described herein and does not set forth any additional current or future obligations or agreements between the parties, except

that the parties may by written amendment amend the scope of this SDA.

XXIV. Joint Responsibilities

Each agency shall ensure staff is conforming to this agreement and applicable state and federal laws and regulations by supervising, auditing, and reviewing procedures. Revisions will be made as needed to ensure adherence.

XXV. CalWIN Confidential Information

By signing below, HHSA grants information of children that are eligible to receive CalFresh to authorized **[BLANK]** staff, and **[BLANK]** accepts the responsibilities for such information as outlined in this agreement and in applicable federal and state laws, regulations, and directives.

XXVII. *Live Well San Diego Vision*

The County of San Diego Health and Human Service Agency agreements support *Live Well San Diego*. *Live Well San Diego* (LWSD), developed by the County of San Diego, is a comprehensive, innovative, regional vision that combines the efforts of partners inside and outside County government to help all residents be healthy, safe, and thriving. All HHSA partners to this agreement, to the extent feasible, are expected to advance this vision, which was implemented in a phased approach. The first phase, *Building Better Health*, was adopted by the Board of Supervisors in 2010, and focuses on improving the health of residents and supporting healthy choices. The second phase, *Living Safely*, seeks to ensure residents are protected from crime and abuse, neighborhoods are safe, and communities are resilient to disasters and emergencies. The third and final phase, *Thriving*, was adopted in 2014 and focuses on promoting a region in which residents can enjoy the highest quality of life.

Information about LWSD can be found on the County's website and a website designated to the vision:
http://www.sdcounty.ca.gov/hhsa/programs/sd/live_well_san_diego/index.html and
http://www.LiveWellSD.org

XXVIII. Term

This SDA shall become effective on the date all of the parties have signed this SDA. This agreement shall continue unless terminated by mutual agreement and/or by state and/or federal directive and/or breach of confidentiality.

XXIX. Termination For Convenience

The County may, by written notice stating the extent and effective date, terminate this SDA for convenience in whole or in part, at any time.

XXX. Counterparts

This SDA may be executed in any number of separate counterparts, each of which shall be deemed an original but all of which when taken together shall constitute one and the same instrument.

XXXI. **[BLANK]** shall comply with the information privacy and security provisions contained in Exhibit B.

Dated: _____ County of San Diego,
Health & Human Services Agency

By: _____

Dated: _____ Other Party

By: _____

EXHIBIT A

INSURANCE REQUIREMENTS

Without limiting Contractor's indemnification obligations to County, Contractor shall provide at its sole expense and maintain for the duration of this Contract, or as may be further required herein, insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of the work by the Contractor, his agents, representatives, employees or subcontractors.

1. Minimum Scope of Insurance

Coverage shall be at least as broad as:

A. Commercial General Liability, Occurrence form, Insurance Services Office form CG0001.

B. Automobile Liability covering all owned, non-owned, hired auto Insurance Services Office form CA0001.

C. Workers' Compensation, as required by State of California and Employer's Liability Insurance.

D. Cyber Security Liability:

2. Minimum Limits of Insurance

Contractor shall maintain limits no less than:

A. Commercial General Liability including Premises, Operations, Products and Completed Operations, Contractual Liability, and Independent Contractors Liability: $1,000,000 per occurrence for bodily injury, personal injury and property damage. The Project Specific Aggregate limit shall be $2,000,000.

B. Automobile Liability: $1,000,000 each accident for bodily injury and property damage.

C. Employer's Liability: $1,000,000 each accident for bodily injury or disease. Coverage shall include a waiver of subrogation endorsement in favor of County of San Diego.

D. Cyber Security Liability: Coverage for both electronic and non-electronic data breach with an aggregate limit of not less than $1,000,000. Coverage shall apply to data breach for Third-Party Liability encompassing judgments or settlement and defense costs arising out of litigation due to a data breach and data breach response costs for customer notification and credit monitoring service fees.

3. Deductibles and Self-Insured Retentions

Any deductible or self-insured retention must be declared to and approved by the County Risk Management. At the option of the County, either: the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the County or the Contractor shall provide a financial guarantee satisfactory to the County guaranteeing payment of losses and related investigations, claim administration and defense expenses.

4. Other Insurance Provisions

The general liability, automobile liability and professional liability policies are to contain, or be endorsed to contain the following provisions:

A. Additional Insured Endorsement (Does not apply to professional liability)
Any general liability policy provided by Contractor shall contain an additional insured endorsement applying coverage to the County of San Diego, the members of the Board of Supervisors of the County and the officers, agents, employees and volunteers of the County, individually and collectively.

B. Primary Insurance Endorsement
For any claims related to this Contract, the Contractor's insurance coverage shall be primary insurance as respects the County, the members of the Board of Supervisors of the County and the officers, agents, employees and volunteers of the County, individually and collectively. Any insurance or self-insurance maintained by the County, its officers, officials, employees, or volunteers shall be excess of the Contractor's insurance and shall not contribute with it.

C. Notice of Cancellation
Notice of Cancellation shall be in accordance with policy provisions.

D. Severability of Interest Clause
Coverage applies separately to each insured, except with respect to the limits of liability, and that an act or omission by one of the named insureds shall not reduce or avoid coverage to the other named insureds.

GENERAL PROVISIONS

5. Qualifying Insurers

All required policies of insurance shall be issued by companies which have been approved to do business in the State of California by the State Department of Insurance, and which hold a current policy holder's alphabetic and financial size category rating of not less than A-, VII according to the current Best's Key Rating guide, or a company of equal financial stability that is approved in writing by County Risk Management.

6. Evidence of Insurance

Prior to commencement of this Contract, but in no event later than the Effective Date of

the Contract, Contractor shall furnish the County with certificates of insurance and amendatory endorsements effecting coverage required by this clause. Contractor shall furnish a summary of the relevant terms, provisions and conditions of the insurance policy to County. Thereafter, copies of renewal certificates and amendatory endorsements effecting coverage shall be furnished to the County within thirty days of the expiration of the coverage. If any of the terms, provisions or conditions as summarized by the County are changed, revised summaries, shall be furnished to County within thirty days of the expiration of the term of any required policy. Contractor shall permit County at all reasonable times to inspect and review any required policies of insurance.

7. Failure to Obtain or Maintain Insurance; County's Remedies

Contractor's failure to provide insurance specified or failure to furnish certificates of insurance, amendatory endorsements, and policy summaries, or failure to make premium payments required by such insurance, shall constitute a material breach of the Contract, and County may, at its option, terminate the Contract for any such default by Contractor provided that the same is not cured within thirty (30) days of Contractor's receipt of notice from the County specifying the nature of the claimed default.

8. No Limitation of Obligations

The foregoing insurance requirements as to the types and limits of insurance coverage to be maintained by Contractor, and any approval of said insurance by the County are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by Contractor pursuant to the Contract, including, but not limited to, the provisions concerning indemnification.

9. Review of Coverage

County retains the right at any time to review the coverage, form and amount of insurance required herein and may request Contractor to obtain insurance reasonably sufficient in coverage, form and amount to provide adequate protection against the kind and extent of risk which exists at the time a change in insurance is required.

10. Self-Insurance

Contractor may, with the prior written consent of County Risk Management, fulfill some of all of the insurance requirements contained in third Contract under a plan of self-insurance. Contractor shall only be permitted to utilized such self-insurance if in the opinion of County Risk Management, Contractor's (i) net worth and (ii) reserves for payment of claims of liability against Contractor, are sufficient to adequately compensate for the lack of other insurance coverage required by this Contract. Contractor's utilization of self-insurance shall not in any way limit liabilities assumed by Contractor under the Contract.

11. Claims Made Coverage

If coverage is written on a "claims made" basis, the Certificate of Insurance shall clearly so state. In addition to the coverage requirements specified above, such policy shall provide that:

A. The policy retroactive date coincides with or precedes Contractor's commencement of work under the Contract (including subsequent policies purchased as renewals or replacements).

B. Contractor will make every effort to maintain similar insurance during the required extended period of coverage following expiration of the Contract, including the requirement of adding all additional insureds.

C. If insurance is terminated for any reason, Contractor shall purchase an extended reporting provision of at least two years to report claims arising in connection with the Contract.

D. The policy allows for reporting of circumstances or incidents that might give rise to future claims.

12. Subcontractors' Insurance

Contractor shall require that any and all Subcontractors hired by Contractor are insured in accordance with this Contract. If any Subcontractors coverage does not comply with the foregoing provisions, Contractor shall defend and indemnify the County from any damage, loss, cost or expense, including attorney fees, incurred by County as a result of Subcontractors failure to maintain required coverage.

(Remainder of this page blank)

EXHIBIT B

ARTICLE 14: INFORMATION PRIVACY AND SECURITY PROVISIONS

A. This Article is intended to protect the privacy and security of specified County information that Contractor may receive, access, or transmit, under this Agreement. The County information covered under this Article consists of:

1. Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); and
2. Personal Information (PI) as defined under the California Civil Code Section 1798.3. Personal information may include data provided to the County by the State of California or by the Social Security Administration; and
3. Personally Identifiable Information (PII) as defined under the Information Exchange Agreement (IEA) between the State of California and the Social Security Administration (SSA), which incorporates the Computer Matching and Privacy Protection Agreement (CMPPA) between the SSA and the State of California's Health and Human Services Agency.

B. This Article consists of the following parts:

1. Article 14.1, Business Associate Agreement, which provides for the privacy and security of PHI as required by HIPAA;
2. Article 14.2, Privacy and Security of PI and PII, which provides for the privacy and security of PI/PII in accordance with:
   a. The Agreement between the County and the State (and thereby the State and the Social Services Administration) with regards to protection of PI and PII. This includes the IEA and the CMPPA to the extent the Contractor accesses, receives, or transmits PI/PII under these Agreements; and
   b. Civil Code Sections 1798.3 and 1798.29, also known as the California Information Practices Act (CIPA). Although CIPA does not apply to the County or its contractors directly, the County is required to extend CIPA terms to contractors if they use County PI/PII to accomplish a function on the County's behalf; and
3. Article 14.3, Data Security Requirements; and
4. Article 14.4, Miscellaneous.

14.1 BUSINESS ASSOCIATE AGREEMENT

14.1.1 Recitals.

14.1.1.1 This Business Associate Agreement ("BAA") constitutes a Business Associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, 42 U.S.C. section 17921 et seq., and their

implementing privacy and security regulations at 45 CFR Parts 160 and 164. These provisions shall hereafter be collectively referred to as "HIPAA."

14.1.1.2 The County of San Diego ("County") wishes to disclose to the Contractor certain information pursuant to the terms of this BAA, some of which may constitute PHI, including PHI in electronic media ("ePHI") under Federal law.

14.1.1.3 As set forth in this BAA, Contractor, hereafter, is the Business Associate of County, acting on County's behalf and providing services, or performing or assisting in the performance of activities on behalf of County, which include creation, receipt, maintenance, transmittal, use or disclosure of PHI. County and Contractor are each a party to this BAA and are collectively referred to as the "parties."

14.1.1.4 The purpose of this BAA 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 HIPAA, including, but not limited to, the requirement that County shall enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in HIPAA.

14.1.2 Definitions. Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms as are defined in 45 Code of Federal Regulations (CFR) section 160.103 and 164.501 (All regulatory references in this BAA are to Title 45 of the CFR unless otherwise specified).

14.1.2.1 "Breach" shall have the same meaning given to such term under HIPAA.

14.1.2.2 "Business Associate" shall have the same meaning as the term under HIPAA, and in reference to the party to this agreement, shall mean the Contractor.

14.1.2.3 "County" shall mean that part of County designated as the hybrid entity subject to the Standards for Privacy of Individually Identifiable Health Information set forth in sections 160 and Part 164, Subparts A and E and those parts of County designated as Business Associates of other entities subject to the Standards for Privacy of Individually Identifiable Health Information set forth in Parts 160 and 164, Subparts A and E.

14.1.2.4 "County PHI" shall have the same meaning as "Protected Health Information" (PHI) below, specific to PHI received from, or created, maintained, transmitted, used, disclosed, or received by Contractor, or its agents, on behalf of County, under this Agreement.

14.1.2.5 "Covered Entity" shall generally have the same meaning as the term "covered entity" at section 160.103, and in reference to the party to this BAA, shall mean County.

14.1.2.6 "Individual" shall have the same meaning as the term ''individual'' in section 164.501 and shall include a person who qualifies as a personal representative in accordance with section 164.502(g).

14.1.2.7 "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in section 164.501 and is limited to information created or received by Contractor from or on behalf of County.

14.1.2.8 "Required by law" shall have the same meaning as the term ''required by law'' in section 164.501.

14.1.2.9 "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

14.1.2.10 "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of County PHI, or interference with system operations in an information system that processes, maintains or stores County PHI.

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

14.1.3 Responsibilities of Contractor.

14.1.3.1 Permitted Uses and Disclosures of County PHI by Contractor. Contractor shall only use County PHI as required by the Contract or as required by Law. Any such use or disclosure shall, to the extent practicable, be limited to the limited data set as defined in section 164.512(2), or if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure in compliance with HIPAA.

14.1.3.1.1 Except as otherwise limited in this Contract, Contractor may use or disclose County PHI on behalf of, or to provide services to, County for the purposes outlined in Exhibit A, if such use or disclosure of PHI would not violate HIPAA if done by County.

14.1.3.1.2 Except as otherwise limited in the Contract, Contractor may use County PHI to provide Data Aggregation services to County as permitted by sections 164.504(e)(2)(i)(B).

14.1.3.2 Prohibited Uses and Disclosures.

14.1.3.2.1 Contractor shall not disclose County PHI to a health plan for payment or health care operations purposes if County 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 HIPAA.

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

14.1.3.3 Safeguards.

14.1.3.3.1 Contractor shall comply with HIPAA regarding any and all operations conducted on behalf of County under this Contract and shall use appropriate safeguards that comply with HIPAA to prevent the unauthorized use or disclosure of County PHI.

14.1.3.3.2 Contractor shall develop and maintain a written information privacy and security program that complies with HIPAA, and that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

14.1.3.4 Security. Contractor shall ensure the continuous security of all computerized data systems and paper documents containing County PHI. These steps shall include, at a minimum:

14.1.3.4.1 Comply with all Standards put forth in Article 14.3, Data Security Requirements;

14.1.3.4.2 Achieve and maintain compliance with HIPAA; and

14.1.3.4.3 Provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies

14.1.3.5 Mitigation of Harmful Effects. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI by Contractor or its agents, including a subcontractor, and/or in violation of the requirements of the Contract.

14.1.3.6 Contractor's Agents and Subcontractors. Contractor shall ensure that any agent, including a subcontractor, to whom it provides County PHI, imposes the same conditions on such agents that apply to Contractor with respect to County PHI under this BAA, and that comply with all applicable provisions of HIPAA, including requirements that such agents implement reasonable and appropriate administrative, physical, and technical safeguards to protect County PHI. Contractor shall incorporate, when applicable, the relevant provisions of this BAA into each subcontract or sub-award to such agents, including the requirement that any security

incidents or breaches of unsecured County PHI be reported to Contractor.

14.1.3.6.1 In accordance with section 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:

14.1.3.6.2 Provide an opportunity for the subcontractor to end the violation and terminate the agreement if the subcontractor does not end the violation within the time specified by County; or

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

14.1.3.7 Availability of Information to County. Contractor shall provide access to County PHI at the request of County, in the time and manner designated by County, pursuant to section 164.526.

14.1.3.7.1 Contractor shall use the forms and processes developed by County for this purpose and shall respond to all requests for access to records requested by County within forty-eight (48) hours of receipt of request by producing records or verifying there are none.

14.1.3.7.2 Contractor shall make internal practices, books, and records relating to the use and disclosure of County PHI received from, or created or received by Contractor on behalf of County available to County, or at the request of County to the Secretary, in a time and manner designated by County or the Secretary.

14.1.3.8 Cooperation with County. Contractor will cooperate and assist County to the extent necessary to ensure County's compliance with the applicable terms of HIPAA, such as, but not limited to:

14.1.3.8.1 Amendment of County PHI. Contractor shall make any required amendment(s) to County PHI that were requested by an Individual, in accordance with HIPAA. Contractor additionally shall make any amendments to County PHI as County directs or agrees to make pursuant to section 164.526. These amendments shall be made in the time and manner designated by County, and in no more than twenty (20) days.

14.1.3.8.2 Documentation of Disclosures. Contractor shall document disclosures of County PHI, respond to a request by an Individual for an accounting of disclosures of County PHI, and make these disclosures available to County or to an Individual at County's request, in accordance with HIPAA, including but not limited to sections 164.528, and 42 USC

section 17935, and in the time and manner designated by County.

14.1.3.8.2.1 If Contractor maintains electronic health records as of January 2009, Contractor shall provide an accounting of disclosures including those for Treatment, Payment, and Healthcare Operations (TPO), effective January 2014. If Contractor acquires electronic health records for County after January 1, 2009, Contractor shall provide an accounting of disclosures, including those for TPO, 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.

14.1.3.8.2.2 The electronic accounting of disclosures shall include the three (3) years prior to the request for an accounting. Contractor shall provide to County or an Individual, in the time and manner designated by County, but no more than sixty (60) calendar days, accounting of disclosures necessary to meet requirements in section 164.528.

14.1.3.9 Access to County PHI. Contractor shall provide Individuals access and copies of their County PHI, as required by HIPAA, to include:

14.1.3.9.1 If the Contractor maintains County PHI in an Electronic Health Record, and an Individual requests a copy of such information in an electronic format, Contractor shall provide the information in an electronic format, as required under HIPAA.

14.1.3.10 Reporting of Unauthorized Use or Disclosure. Contractor shall implement reasonable systems for the discovery of and prompt reporting to County of any use or disclosure, or suspected use or disclosure, of County PHI not provided for by the Contract and/or any transmission of unsecured County PHI, and to take the following steps.

14.1.3.10.1 Contractor shall provide all reports of Unauthorized Uses or Disclosures simultaneously to County Contracting Officer's Representative and Agency Privacy Officer.

14.1.3.10.2 Initial Report.

14.1.3.10.2.1 Contractor shall notify County immediately by telephone call plus email upon the discovery of a breach of unsecured County PHI in electronic media or in any other media

if County PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the Social Security Administration.

14.1.3.10.2.2 Contractor shall notify County by email within twenty-four (24) hours of the discovery of any suspected security incident or breach of County PHI in violation of this BAA, or potential loss of confidential data affecting this BAA.

14.1.3.10.2.3 A suspected security incident or breach shall be treated as discovered by Contractor as of the first day the breach or security incident is known, even if it is not confirmed, or by exercising reasonable diligence would have known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

14.1.3.10.2.4 Reporting shall additionally include emailing of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall use the most current version of this form, which is posted on County's website, www.cosd.compliance.org.

14.1.3.10.3 Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PHI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

14.1.3.10.4 Investigation and Investigation Report. Contractor shall immediately investigate such security incident, breach, or unauthorized access, use or disclosure of County PHI. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report."

14.1.3.10.5 Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of

the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on County's "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 and applicable 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 County requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and approve the determination of whether a breach occurred, Individual notifications are required, and the corrective action plan is adequate.

14.1.3.10.6 Responsibilities for Notification of Breaches. If County determines that the cause of a breach of County PHI is attributable to Contractor or its subcontractors, agents or vendors, Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under Federal or State 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 requirements that:

14.1.3.10.6.1 Notifications be made to Individuals without unreasonable delay and in no event later than sixty (60) calendar days from the date the breach was discovered. County shall approve the time, manner and content of any such notifications before notifications are made.

14.1.3.10.6.2 Notifications be made to media outlets and to the Secretary, if a breach of unsecured County PHI involves more than five-hundred (500) residents of the State of California or its jurisdiction. County shall approve the time, manner and content of any such notifications before notifications are made.

14.1.3.11 Designation of Individuals.

14.1.3.11.1 Contractor shall designate a Privacy Officer to oversee its data privacy program who shall be responsible for carrying out the requirements of this

section and for communicating on Privacy matters with County.

14.1.3.11.2 Contractor 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 County.

14.1.4 Responsibilities of County.

14.1.4.1 County shall provide Contractor with the Notice of Privacy Practices that County produces in accordance with section 164.520, as well as any changes to such notice.

14.1.4.2 County shall provide Contractor with any changes in, or revocation of, permission by Individual to use or disclose County PHI, if such changes affect Contractor's permitted or required uses and disclosures.

14.1.4.3 County shall notify Contractor of any restriction to the use or disclosures of County PHI that County has agreed to in accordance with section 164.522.

14.1.4.4 County shall not request Contractor to use or disclose County PHI in any manner that would not be permissible under HIPAA if done by County.

14.2 PRIVACY AND SECURITY OF PERSONAL INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

14.2.1 Recitals.

14.2.1.1 In addition to the Privacy and Security Rules under HIPAA, the County is subject to various other legal and contractual requirements with respect to the Personal Information (PI) and Personally Identifiable Information (PII) it maintains. These include the:

14.2.1.1.1 California Information Practices Act (CIPA) of 1977 (California Civil Code section 1798, et. seq.);

14.2.1.1.2 The Agreement between the Social Security Administration (SSA) and the State of California, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency; and

14.2.1.1.3 Title 42 Code of Federal Regulations, Chapter 1, Subchapter A, Part 2.

14.2.1.2 The purpose of this Article 14.2 is to set forth Contractor's Privacy and Security obligations with respect to PI and PII that the Contractor may create, receive, maintain, use, or disclose for or on behalf of County pursuant to this Agreement. Specifically, this Article applies to PI and PII which is not Protected Health Information (PHI), as defined by HIPAA and therefore is not addressed in Article 14.1, the Business Associate Agreement of this Contract. To the extent that data is both PHI and PI, or both PHI and PII, both Sections 14.1 and 14.2 apply.

14.2.1.3 The IEA Agreement requires County to extend the IEA's terms to contractors who receive data provided to County from the SSA, or data provided to County from the SSA through the State of California. If contractor receives such data from County, Contractor must comply with the IEA Agreement.

14.2.2 Definitions. The terms used in this Article 14.2 shall have the same meaning as those terms have in the above referenced statues and agreements. Any reference to statutory, regulatory, or contractual language shall be to such language currently in effect or as amended.

14.2.2.1 "Breach" shall have the same meaning given to such term under the IEA and CMPPA. It shall include a "PII loss," as defined in the CMPPA, and both a "Breach of the security of the system" and a "Notice Triggering Personal Information" event, as identified in CIPA (Civil Code section 1798.29).

14.2.2.2 "County" shall mean that part of County designated as the hybrid entity, subject to the Standards for Privacy of Individually Identifiable Health Information set forth in and those parts of County designated as Contractors of other entities subject to the Standards for Privacy of Individually Identifiable Health Information, as set forth in Part 160 and Part 164, Subparts A and E.

14.2.2.3 "County PII/PI" shall have the same meaning as Personally Identifiable Information/Personal Information as below, specific to PII/PI received by Contractor from County or acquired or created by Contractor in connection with performing the functions, activities, and services specified in this Article 14.2 on behalf of County.

14.2.2.4 "Individual" shall generally have the same meaning as the term ''individual'' in Title 45 Code of Federal Regulations, Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

14.2.2.5 "Personal Information" shall have the same meaning given to such term in CIPA, section 1798.3(a).

14.2.2.6 "Personally Identifiable Information" (PII) shall have the same meaning given to such term in the IEA and the CMPPA.

14.2.2.7 "Required by law" shall have the same meaning as the term ''required by law'' in 45 CFR section 164.501.

14.2.2.8 "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of County PII/PI, or confidential data, or interference with system operations of an information system.

14.2.3 Responsibilities of Contractor.

14.2.3.1 Permitted Uses and Disclosures of County PII/PI by Contractor. Contractor shall only use County PII/PI to perform functions, activities, or services for or on behalf of County pursuant to this Contract, provided that such use or disclosure does not violate any applicable Federal or State law or regulation.

14.2.3.1.1 Confidentiality of Alcohol and Drug Abuse records. Contractor shall comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter 1, Subchapter A, Part 2, as applicable.

14.2.3.2 Prohibited Uses and Disclosures. Contractor shall not use or disclose County PII/PI, other than as permitted or required by the Contract or as permitted or required by Law.

14.2.3.3 Safeguards.

14.2.3.3.1 Contractor shall use appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of County PII/PI and to prevent use or disclosure of County PII/PI, other than as provided for by this Contract.

14.2.3.3.2 Contractor shall develop and maintain a written information privacy and security program that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

14.2.3.4 Security. Contractor shall take any and all steps necessary to ensure the continuous safety of all data systems containing County PII/PI. The Contractor shall, at a minimum:

14.2.3.4.1 Comply with all of the data system security precautions listed in Article 14.3, Data Security Requirements;

14.2.3.4.2 Provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

14.2.3.4.3 If the data includes County PII, Contractor shall also comply with the Privacy and Security requirements in the CMPPAA and the IEA.

14.2.3.5 Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PII/PI by Contractor or its agents, in violation of this Article 14.2.

14.2.3.6 Contractor's Agents or Subcontractors. Contractor shall ensure that any agent, including a subcontractor that creates, receives, maintains, or transmits County PII/PI on behalf of the Contractor shall adhere to the same restrictions, conditions, and requirements that apply to the Contractor. Contractor shall incorporate, when applicable, the relevant provisions of this Article 14.2 into each subcontract or sub-award to such agents, subcontractors and vendors, including the requirements related to security incidents or breaches of unsecured County PII/ PI.

14.2.3.7 Availability of Information. Contractor shall make County PII/PI available to County for purposes of oversight, inspection, amendment, and response to request for records, injunctions, judgments, and orders for production of County PII/PI. Contractor shall provide a list of all employees, contractors and agents who have access to County PII/PI, including employees, and agents of its subcontractors and agents, at the request of County. Contractor shall provide any requested records to County within forty-eight (48) hours of such request.

14.2.3.7.1 Internal Practices. Contractor shall make internal practices, books, and records relating to the use and disclosure of County PII/PI received from, or created or received by Contractor on behalf of County available to County, in a time and manner designated by County. Confidentiality shall not prevent County, its agents, or any other governmental entity from accessing such records if that access is legally permissible under the applicable Federal or State regulations.

14.2.3.8 Cooperation with County. Contractor will cooperate and assist County, in the time and manner designated by County, to ensure County's compliance with applicable Federal and State laws and regulations, such as, but not limited to CIPA. Contractor's cooperation shall include, but is not limited to: accounting of disclosures, correction of errors, production, disclosures of a security breach, and notice of such breach to affected individuals that involve County PII/PI and Contractor.

14.2.3.9 Reporting of Breaches and Security Incidents. Contractor shall implement reasonable systems for the discovery of, prompt

reporting to County of, and prompt corrective action regarding any use or disclosure, or suspected use or disclosure, of County PII/PI not provided for by the Contract and/or any transmission of unsecured County PII/PI and shall take the following steps.

14.2.3.9.1 Contractor shall make all reporting of breaches and security incidents simultaneously to County Contracting Officer's Representative and Agency Privacy Officer.

14.2.3.9.2 Initial Reporting.

14.2.3.9.2.1 Reporting shall be immediate, by both telephone and email, upon the discovery of a breach of unsecured County PII/PI in electronic media or in any other media if County PII/PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the Social Security Administration.

14.2.3.9.2.2 Reporting shall be within twenty-four (24) hours by email of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/ PI in violation of this Article 14.2, or potential loss of confidential data affecting this Article 14.2.

14.2.3.9.2.3 A breach or suspected security incident shall be treated as discovered by Contractor as of the first day on which the breach is known, even if not confirmed, 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 the Contractor.

14.2.3.9.2.4 Reporting shall additionally include emailing of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall use the most current version of this form, which is posted on County's website, www.cosd.compliance.org.

14.2.3.9.3 Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/PI, Contractor

shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

14.2.3.9.4 Investigation and Investigation Report. Contractor shall immediately investigate such security incident or breach. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report."

14.2.3.9.5 Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on County's "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 Federal and 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 County requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and approve the determination of whether: a breach occurred, individual notifications are required, and the corrective action plan is adequate.

14.2.3.9.6 Responsibility for Reporting Breaches. If County determines that the cause of a breach of County PII/PI is attributable to Contractor or its subcontractors, agents or vendors, Contractor is responsible for all required reporting as specified under CIPA section 1798.29(a) and as may be required under IEA, as well as any other Federal or State law and shall pay any costs of such notifications, as well as any costs associated with the breach. County shall approve the time, manner, and content of any such notifications and County's review and approval must be obtained before the notifications are made. If the Contractor believes duplicate reporting of the same breach or incident may occur, because its subcontractors or agents may report the breach or incident to County as well, Contractor shall notify County and may take action to prevent duplicate reporting.

14.2.3.10 Designation of Individuals. Contractor shall appoint Privacy and Security officials who are accountable for compliance with this Article and for communicating Privacy and Security matters to County.

14.3 DATA SECURITY REQUIREMENTS

Contractor shall ensure the continuous security of all computerized data systems and paper documents containing County PHI and/or County PII/PI. These steps shall include, at a minimum:

14.3.1 Personnel Controls. Contractor shall ensure: all workforce members who assist in the performance of functions or activities on behalf of County, or access or disclose County PHI and/or County PII/PI, shall:

14.3.1.1 Have undergone a thorough Contractor background check, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security, privacy, or integrity of County PHI and/or County PII/PI, prior to the workforce member obtaining access to County PHI and/or County PII/PI. The Contractor shall retain each workforce member's Contractor background check documentation for a period of three (3) years following contract termination.

14.3.1.2 Complete privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training shall sign a certification, indicating the workforce member's name and the date on which the training was completed. These certifications shall be retained for a period of six (6) years following contract termination, and shall be available to County upon request. Sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to County PHI and/or County PII /PI and shall be renewed annually. The Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following contract termination.

14.3.1.3 Be appropriately sanctioned if they fail to comply with security and privacy policies and procedures, including termination of employment when appropriate.

14.3.2 Physical Security Controls. Contractor shall safeguard County PHI and/or County PII/PI from loss, theft, inadvertent disclosure, and therefore shall:

14.3.2.1 Ensure County PHI and/or County PII/PI is used and stored in an area that is physically safe from access by unauthorized persons during both working hours and nonworking hours;

14.3.2.2 Secure all areas of Contractor facilities where Contractor workers use or disclose County PHI and/or County PII/PI. The Contractor shall

ensure that these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or other access authorization, and access to premises is by official identification;

14.3.2.3 Issue workers who assist in the administration of County PHI and/or County PII/PI identification badges and require workers to wear badges at facilities where County PHI and/or County PII/PI is stored or used;

14.3.2.4 Ensure each location where County PHI and/or County PII/PI is used or stored has procedures and controls that ensure an individual whose access to the facility is terminated:

14.3.2.4.1 Is promptly escorted from the facility by an authorized employee; and

14.3.2.4.2 Immediately has their access revoked to any and all County PHI and/or County PII/PI.

14.3.2.5 Ensure there are security guards or a monitored alarm system twenty-four (24) hours a day, seven (7) days a week at facilities where County PHI and/or County PII/PI is stored;

14.3.2.6 Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI and/or County PII/PI have perimeter security and access controls that limit access to only authorized Information Technology Staff. Visitors to the data center area must be escorted by authorized IT staff at all times;

14.3.2.7 Store paper records with County PHI and/or County PII/PI in locked spaces in any facilities that are multi-use, meaning that there are County PHI and/or County PII/PI functions and Contractor functions in one building in work areas that are not securely segregated. The contractor shall have policies that state workers shall not leave records with County PHI and/or County PII/PI unattended at any time in cars or airplanes and shall not check County PHI and/or County PII/PI on commercial flights; and

14.3.2.8 Use all reasonable means to prevent non-authorized personnel and visitors from having access to, control of, or viewing County PHI and/or County PII/PI.

14.3.3 Technical Controls. Contractor shall ensure:

14.3.3.1 All workstations, copiers, and laptops that process and/or store County PHI and/or County PII/PI shall:

14.3.3.1.1 Be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk; and

14.3.3.1.2 Install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

14.3.3.2 Have critical security patches applied, with system reboot if necessary. There shall be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. All applicable patches shall be installed within thirty (30) days of vendor release.

14.3.3.3 All servers containing unencrypted County PHI and/or County PII/PI shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

14.3.3.4 Only the minimum necessary amount of County PHI and/or County PII/PI required to perform necessary business functions may be copied, downloaded, or exported.

14.3.3.5 All electronic files that contain County PHI and/or County PII/PI shall be encrypted when stored on any removable media or portable device (i.e. flash drives, cameras, mobile phones, CD/DVD, backup media, etc). Encryption shall be a FIPS 140-2 certified algorithm, which is 128bit or higher, such as AES.

14.3.3.6 All users shall be issued a unique user name for accessing County PHI and/or County PII/PI. Username shall be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours.

14.3.3.6.1 Passwords shall be:

14.3.3.6.1.1 At least eight characters;

14.3.3.6.1.2 A non-dictionary word;

14.3.3.6.1.3 Changed at least every ninety (90) days;

14.3.3.6.1.4 Changed immediately if revealed or compromised; and

14.3.3.6.1.5 Composed of characters from at least three of the following four groups from the standard keyboard:

14.3.3.6.1.5.1 Upper case letters (A-Z)

14.3.3.6.1.5.2 Lower case letters (a-z)

14.3.3.6.1.5.3 Arabic numerals (0-9)

14.3.3.6.1.5.4 Non-alphanumeric characters (punctuation symbols)

14.3.3.6.2 Passwords shall not be shared and shall not be stored in readable format on the computer.

14.3.3.7 Appropriate management control and oversight, in conjunction with County of the function of authorizing individual user access to County

PHI and/or County PII/PI and over the process of maintaining access controls numbers and passwords.

14.3.3.8 When no longer needed, all County PHI and/or County PII/PI shall 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.

14.3.3.9 All systems providing access to, transport of, or storage of County PHI and/or County PII/PI shall:

14.3.3.9.1 Provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

14.3.3.9.2 Display a warning banner stating that data is confidential systems are logged and system use is for business purposes only by authorized users. Users must be directed to log off the system if they do not agree with these requirements.

14.3.3.9.3 Maintain an automated audit trail that identifies the user or system process which initiates a request for County PHI and/or County PII/PI, or which alters County PHI and/or County PII/ PI. The audit trail shall be date and time stamped, shall log both successful and failed accesses, shall be read only, and shall be restricted to authorized users. If County PHI and/or County PII/ PI is stored in a database, database logging functionality shall be enabled. Audit trail data shall be archived for at least three (3) years after occurrence, and shall be available to County upon request.

14.3.3.9.4 Use role based access controls for all users, enforcing the principle of least privilege.

14.3.3.9.5 Be protected by a comprehensive intrusion detection and prevention solution if they are accessible via the internet.

14.3.3.10 All data transmissions of County PHI and/or County PII/PI outside the secure internal network shall 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 County PHI and/or County PII/PI can be encrypted. This requirement pertains to any type of County PII/PI in motion such as website access, file transfer, and E-Mail.

14.3.4 Audit Controls. Contractor shall ensure:

14.3.4.1 All systems processing and/or storing County PHI and/or County PII/PI shall 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.

14.3.4.2 All systems processing and/or storing County PHI and/or County PII/PI shall have a routine procedure in place to review system logs for unauthorized access.

14.3.4.3 All systems processing and/or storing County PHI and/or County PII/PI shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

14.3.4.4 Investigate anomalies in usage of County PHI and/or County PII/PI identified by County and report conclusions of such investigations and remediations to County.

14.4.4 Business Continuity / Disaster Recovery Controls

14.4.4.1 Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic County PHI and/or County PII/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 twenty-four (24) hours.

14.4.4.2 Contractor shall ensure Data Centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI or PII/PI, must include sufficient environmental protection such as cooling, power, fire prevention, detection, and suppression.

14.4.4.3 Contractor shall have established documented procedures to backup County PHI and/or County PII/PI to maintain retrievable exact copies of County PHI and/or County PII/PI. The plan shall 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 County PHI and/or County PII/PI should it be lost. At a minimum, the schedule shall be a weekly full backup and monthly offsite storage of County data.

14.3.5 Paper Document Controls. Contractor shall ensure:

14.3.5.1 County PHI and/or County PII/PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or separate office inside a larger office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI and/or County PII/PI in paper form shall not be left unattended at any time in vehicles and shall not be checked in baggage during commercial flights.

14.3.5.2 Visitors to areas where County PHI and/or County PII/PI are contained shall be escorted and County PHI and/or County PII/PI shall be kept out of sight while visitors are in the area.

14.3.5.3 County PHI and/or County PII/PI shall be disposed of through confidential means, such as cross cut shredding and pulverizing.

14.3.5.4 County PHI and/or County PII/PI shall not be removed from the premises of the Contractor except for identified routine business purposes or with express written permission of County.

14.3.5.5 Faxes containing County PHI and/or County PII/PI shall not be left unattended and fax machines shall be in secure areas. Fax cover sheets shall contain a confidentiality statement instructing persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

14.3.5.6 Mailings of County PHI and/or County PII/PI shall be sealed and secured from damage or inappropriate viewing of County PHI and/or County PII/PI to the extent possible. Mailings which include 500 or more individually identifiable records of County PHI and/or County PII/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 County's HHSA Privacy Officer to use another method is obtained.

14.3.5.7 Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI and/or County PII/PI by Contractor or its agents, including a subcontractor, and/or in violation of the requirements of the Contract.

14.4 MISCELLANEOUS

14.4.1.1.1 Disclaimer. County makes no guarantee that compliance with this agreement will be satisfactory for the Contractor's own purposes.

14.4.1.1.2 Amendment. The Parties agree to take action as necessary to amend this Article 14 from time to time as is necessary for County to comply with the requirements of any and all applicable other Federal or State laws and regulations.

14.4.1.1.3 Judicial or Admin Proceedings. Contractor will notify County if it is named as a defendant in any criminal, civil, or administrative proceeding for a violation of any applicable security or privacy law.

14.4.1.1.4 Assistance in Litigation or Admin Proceedings. Contractor shall make itself and any of its agents available, at no cost to County, to testify, or otherwise, in the event of litigation or administrative proceedings commenced against County, its directors, officers, or employees, based on claimed violations of any applicable confidentiality, privacy, or security law or regulation, whether Federal or State, if that litigation or proceeding involves actions of Contractor or its agents, except those where Contractor or its Agents are named as an adverse party.

14.4.1.1.5 Interpretation. Any ambiguity in this Article 14 shall be resolved in favor of a meaning that permits County to comply with the applicable Federal or State law or regulation.

14.4.1.1.6 Conflict. If a conflict between any of the standards contained in any of these enumerated sources of standards is found, Contractor shall follow the most stringent standard. The most stringent means that safeguard which provides the highest level of protection to County PHI and/or County PII/PI from unauthorized disclosure.

14.4.1.1.7 Regulatory References. All references in this Article 14 to any regulation or law mean the regulation or law currently in effect, including those legal and regulatory changes that occur after the effective date of this Agreement.

14.4.1.1.8 Survival. The respective rights and obligations of Contractor and Contractor under this Article 14 shall survive the termination of the Contract.

14.4.1.1.9 No Waiver of Obligations. No change, waiver, or discharge of any liability or obligation hereunder or 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, an any other occasion.

14.4.1.1.10 Due Diligence. Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Article 14 and is in compliance with all applicable Federal and State laws and regulations, and that its agents, subcontractors, and vendors are in compliance with their obligations as required by this Article 14.

14.4.1.1.11 Effect of Termination. Upon termination of the Contract, for any reason, with respect to any and all County PHI and/or County PII/PI received from County, or created or received by Contractor on behalf of County:

14.4.1.1.11.1 Contractor shall return or destroy all County PHI and/or County PII/PI and retain no copies of County PHI and/or County PII/PI, except County PHI and/or County PII/PI necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities, as mutually agreed upon by the Parties.

14.4.1.1.11.2 Upon mutual agreement of the Parties that return or destruction of County PHI and/or County PII/PI is infeasible, Contractor shall extend the protections of this Article to such County PHI and/or County PII/PI for so long as Contractor maintains such County PHI and/or County PII/PI.

14.4.1.1.11.3 Contractor shall return to County or destroy, as determined by County, County PHI and/or County PII/PI retained by Contractor when it is no longer needed by Contractor for its proper management and administration or to carry out its legal responsibilities.

14.4.1.1.11.4 This provision shall apply to County PHI and/or County PII/PI that is in the possession of subcontractors or agents of Contractor.