

# **CONTRACT NAME: MEMORANDUM OF UNDERSTANDING BETWEEN THE COUNTY OF YOLO AND DAVIS JOINT UNIFIED SCHOOL DISTRICT**

**BRIEF DESCRIPTION OF CONTRACT:** This Memorandum of Understanding between the County of Yolo and DJUSD is to establish a data sharing agreement to identify potential National School Lunch Program youth participants and Yolo County families that may be eligible for CalFresh.

This MOU establishes a framework for DJUSD and the Health & Human Services Agency to share specified data under Welfare and Institutions Code section 18901.55 and Education Code sections 49557.3 and 49558, which permit a school district and the local agency that determines CalWORKs and CalFresh program eligibility to share information, with participant consent, to help identify clients eligible for CalFresh and the National School Lunch Program.

Sharing the data will allow Yolo County to identify greater numbers of potential DJUSD families in need of the free and reduced lunch program and will allow the District to provide additional services and programs for eligible students.

## **MOU No. 17-24**

### **CALWORKS AND CALFRESH FREE AND REDUCED LUNCH DATA SHARING MEMORANDUM OF AGREEMENT**

This Memorandum of Understanding (MOU) is entered into as of the date the Agreement is fully executed, between the County of Yolo, a political subdivision of the State of California, for the benefit of the Yolo County Health and Human Services Agency (HHSA), and the Davis Joint Unified School District (District).

The purpose of this MOU is to establish a data sharing agreement to identify potential National School Lunch Program (NSLP) youth participants and Yolo County families that may be eligible for CalFresh. This MOU establishes a framework for District and HHSA to share specified data under Welfare and Institutions Code section 18901.55 and Education Code sections 49557.3 and 49558, which permit a school district and the local agency that determines CalWORKs and CalFresh program eligibility to share information, with participant consent, to help identify clients eligible for CalFresh and the NSLP.

#### **ARTICLE I FRAMEWORK FOR DATA SHARING**

##### **A. Requirements for CalWORKs and CalFresh Match Local Educational Agencies (LEA)**

1. HHSA may share with District information provided on the CalWORKs and CalFresh program applications of clients who meet potential eligibility criteria for NSLP, are enrolled in the County's CalWORKs and CalFresh programs and are currently living within District boundaries. Those who: (a) do not currently receive NSLP benefits, (b) are members of households with incomes that do not exceed 133 percent of the federal poverty level for their household size and (c) are not currently participating in any other assistance program will be considered a "project-match". Those so indicated by the match shall confirm eligibility for federal school meal programs. This information is to identify youth only attending said school districts who may be direct certified for Free and Reduced Lunch.
2. HHSA will forward the information by either hand delivering or emailing the data to the District-assigned representative.
3. The parties acknowledge that the CalWORKs and CalFresh program applications are confidential and, with the exception of forwarding the information on the application for use in Free and Reduced Lunch program enrollment consistent with this MOU, the parties shall not share the information with any other governmental agency, including the federal United States Citizenship and Immigration Services and the Social Security Administration, or use the information for any purpose other than enrollment in the Free and Reduced Lunch program.

4. After HHSA shares information provided on a CalWORKs or CalFresh program application with District for the purpose of determining the applicant's eligibility for the Free and Reduced Lunch Program, District and HHSA may not share information about the applicant or his/her household with each other, or any entity, unless specifically authorized to do so pursuant to other provisions of law.

#### **5. District Responsibilities**

- a. District shall use the information provided on a CalWORKs or CalFresh program application only for purposes directly related to the enrollment of families in the Free and Reduced Lunch Program
- b. District will review Free and Reduced Lunch referrals made by HHSA and will take no further action if the household is determined to already have an active Free and Reduced Lunch application.
- c. District will make a timely determination of Free and Reduced Lunch eligibility and benefits and will provide adequate notice of case determination.
- d. District shall reiterate to the household that no information will be shared with any other governmental agency, including the United States Citizenship and Immigration Services and the Social Security Administration, or use the information for any purpose other than enrollment in the Free and Reduced Lunch program.

#### **B. Requirements for NSLP Sharing with HHSA**

1. District may share information provided on the NSLP application with HHSA if the child is approved for free or reduced price meals and the applicant consents to the sharing of that information.
2. The parties agree to use the following process to share the information. In the beginning of each school year, but in no event later than September 30, District will forward the NSLP applications and the signed consent form to HHSA provided the child is approved for free or reduced price meals and the applicant consents to the sharing of that information. The information may be shared by either hand delivering or emailing the data from District to the HHSA-assigned representative.
3. The parties acknowledge that the NSLP application is confidential and, with the exception of the forwarding the information on the application for use in CalFresh program enrollment consistent with this MOU, the parties shall not share the information with any other governmental agency, including the federal United States Citizenship and Immigration Services and the Social Security Administration, or use the information for any purpose other than enrollment in the CalFresh program.
4. The parties acknowledge that the National School Lunch Act establishes a fine of not more than \$1,000 or imprisonment of not more than 1 year, or both, if any eligibility

information is published, divulged, disclosed, or made known in any manner or extent not authorized by federal law. The parties further acknowledge that United States Code 5 USC 552a(i) establishes a fine of not more than \$5,000 for any employee who willfully discloses confidential material in any manner to any person or agency not entitled to receive it, or who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses.

5. After District shares information provided on a NSLP application with HHSA for the purpose of determining the applicant's eligibility for the CalFresh program, District and HHSA shall not share information about the applicant or his/her household with each other, or any entity, unless specifically authorized to do so pursuant to other provisions of law.
6. The parties acknowledge that any NSLP applicant whose information is shared with the local CalFresh agency will be required to complete a CalFresh application prior to enrollment in the CalFresh program.

#### **7. District Responsibilities**

- a. District will continue to make applications for Free or Reduced Price meals through the NSLP available to all students, pursuant to Education Code section 49557. The NSLP applications will give parents/guardians an option to consent to sharing information provided on the application with HHSA for purposes directly related to the enrollment of the CalFresh program. The application materials provided by District to students shall state that participation in the CalFresh program is entirely voluntary and that the CalFresh agency will provide the applicant with a CalFresh application for the purposes of enrollment in the CalFresh program.
- b. District will forward the information provided on the NSLP application to HHSA provided the child is approved for Free or Reduced Price meals and the applicant consents to the sharing of that information.
- c. District shall continue to ensure that all applications and records concerning any individual made or kept by District in connection with administration of the free or reduced price meal and CalFresh eligibility are confidential, as required by Education Code section 49558.

#### **8. HHSA Responsibilities**

- a. HHSA shall use the information provided on a NSLP application only for purposes directly related to the enrollment of families in the CalFresh Program
- b. HHSA will review CalFresh referrals made by District and will take no further action if the household is determined to already have an active CalFresh case.

- c. HHSA will make contact with the referred household to make an appropriate determination of CalFresh program eligibility. HHSA will treat the NSLP application as a written request for a CalFresh application. HHSA will request additional information pertinent to the household if necessary to make an eligibility determination.
- d. HHSA will make a timely determination of CalFresh eligibility and benefits and will provide adequate notice of case determination after a signed application for CalFresh is received.
- e. HHSA shall reiterate to the household that no information will be shared with any other governmental agency, including the United States Citizenship and Immigration Services and the Social Security Administration, or use the information for any purpose other than enrollment in the CalFresh program.

## **ARTICLE II**

### **STATUTES, REGULATIONS AND POLICIES**

#### **A. COMPLIANCE WITH STATUTES AND REGULATIONS**

- 1. Both parties will comply with all Federal, State and local statutes, laws, rules, regulations, codes, and ordinances effective at the inception of the MOU and that become effective during the term of this MOU relating to its performance under this MOU. To the extent that laws are in conflict with provisions of this MOU, the laws shall prevail. Each party will also provide services under the MOU in accordance with the resolutions, policies, procedures, directives and guidelines issued by the County Board of Supervisors or School Board of Trustees.
- 2. Each party will comply with all applicable subsequent amended or added Federal, State, and local laws and execute amendments necessary to implement such laws.

#### **B. NONDISCRIMINATION OF EMPLOYMENT**

- 1. Both parties shall comply with all applicable Federal, State, and local laws and regulations including policies concerning nondiscrimination and equal opportunity in contracting. Such laws include but are not limited to the following: Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; The Rehabilitation Act of 1973 (Sections 503 and 504); California Fair Employment and Housing Act (Government Code sections 12900 et seq.); and California Labor Code sections 1101 and 1102.
- 2. During the performance of this MOU, each party and its subcontractors must not unlawfully discriminate, harass or allow harassment, against any employee or

applicant for employment because of:

- a. Age (40 and above),
  - b. Ancestry,
  - c. Color,
  - d. Disability (Mental and Physical) including HIV and AIDS,
  - e. Ethnic Group Identification,
  - f. Family and Medical Care Leave,
  - g. Marital Status,
  - h. Medical Condition (cancer/genetic characteristics),
  - i. National Origin,
  - j. Pregnancy Disability Leave,
  - k. Political Belief,
  - l. Race,
  - m. Reasonable Accommodation,
  - n. Religious Creed,
  - o. Sex/Gender, or
  - p. Sexual Orientation.
3. Each party and its subcontractors will ensure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment.
4. Each party and its subcontractors will comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12900 et seq.) and the applicable regulations promulgated hereunder (California Code Regulations, Title 2, Section 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code, Section 12990 (a) - (f), are incorporated into this MOU by reference and made a part hereof as if set forth in full (California code Regulations, Title 2, Section 7285.0 et seq.).
5. Each party and its subcontractors will give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.
6. Each party must include the non-discrimination and compliance provisions of this clause in all subcontractors to perform work under this MOU.

**C. NONDISCRIMINATION OF SERVICES**

1. Each party will ensure that services provided under this MOU are nondiscriminatory and that no person is denied services or subjected to discrimination under any program or activity as identified in Paragraph B (2), except the following:
  - a. Family and Medical Care Leave, and
  - b. Pregnancy Disability Leave

2. Both parties may exclude an individual or group when the services of a program are restricted to a specific class of individuals or group and included as a provision of this MOU.
3. Each county will ensure that its appropriate personnel involved in providing services are educated regarding AIDS and HIV infection.

#### **D. CONFIDENTIALITY**

1. The use or disclosure of information concerning CalWORKs and CalFresh applicants and recipients will be limited to use by designated District staff for the items listed below. Information will not be released to any other agencies except in accordance with Welfare & Institutions Code sections 10850, 10850.2 and 14100.2. These records fall within the description of confidential records. District recognizes that unauthorized release of confidential information may constitute a misdemeanor under Welfare & Institutions Code sections 10850 or 14100.2 and result in individual criminal or civil liability. The Welfare & Institutions code sections 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 Welfare & Institutions code section 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." District may only use confidential records provided by HHSA under this MOU as follows:
  - a. Utilize information provided by HHSA from CalWIN to identify children who are in households that receive CalWORKs or CalFresh to confirm eligibility for a free or reduced-price school lunch/breakfast.
    - 1) District will provide HHSA a list of employees designated to access CalWIN data specified above.
    - 2) District 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.
    - 3) District acknowledges that clearances made through the match shall be used only to identify children who are in households that receive CalWORKs or CalFresh to confirm eligibility for a free or reduced-price school lunch/breakfast.
    - 4) District agrees that designated employees will not access their own case assistance data or those of any friend, relative, business relation, personal acquaintance or other person that may know.
    - 5) In the event of any unauthorized access to or improper use of confidential data, District shall immediately notify HHSA and take disciplinary action against the employee making or allowing the unauthorized disclosure, up to and including termination. District shall notify HHSA when an employee is subject to such disciplinary action.

- 6) District agrees that all individually identifiable information received from HHSA under this MOU will be destroyed by shredding or a similar method of destruction once the use for the information has ended.
  - 7) District 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 MOU are being met.
  - 8) District shall not release any individual identifying information to anyone not a designated employee under this MOU or as otherwise allowed by Welfare and Institutions Code sections 10850 or 14100.2. This information may be released under Welfare and Institutions Code section 10850.2 if a properly executed written release of information is obtained by HHSA or District. Any written releases obtained by District must be maintained in a file for audit purposes.
  - 9) District 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 Welfare and Institutions Code sections 10850, 10850.2 and 14100.2. District must provide a copy of a Summary of Policy to HHSA three days before the designated staff member accesses the information.
  - 10) District agrees to provide updates to HHSA within ten business days for any designated staff for whom access is being deleted or work location is being changed.
2. Strict adherence to the criteria stated in items 1 through 10 must be followed. Confidential client information may only be accessed by designated staff when the applicable conditions stated in items 1 through 10 have been met.
  3. Each party will inform all employees, agents, officers, and all persons performing services at its direction of the above provisions. All provisions of Article II, Section D survive the termination of this MOU.

### **ARTICLE III**

#### **GENERAL TERMS**

##### **1. TERM**

This term of this MOU will begin on the date the MOU is fully executed and terminate on the anniversary date three years later.

##### **2. TERMINATION**

Either party may terminate this MOU by giving 30 day written notice of termination to the other party.

##### **3. INDEMNITY**

Each party shall indemnify, defend, protect, hold harmless, and release the other, their elected bodies, officers, agents, and employees, from and against any and all claims,



losses, proceedings, damages, causes of action, liability, costs, or expense (including attorneys' fees and witness costs) arising from or in connection with, or caused by any negligent act or omission or willful misconduct of such indemnifying party arising from this MOU. This indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages or compensation payable to or for the indemnifying party under workers' compensation acts, disability benefit acts, or other employee benefit acts.

**4. AVAILABILITY OF FUNDS**

All provisions of this MOU are subject to the continued appropriation and availability of funds to both agencies for the services and resources outlined. In the event that funds, staffing or resources are no longer available, the parties unilaterally may take appropriate actions including, but not limited to, reducing existing service authorization, or immediate termination of the MOU.

**5. SUBCONTRACTING AND ASSIGNABILITY**

This MOU cannot be subcontracted or assigned without prior written approval of the other party. In the event of such approval, any subcontract or assignment is subject to the same terms as provided under this MOU. The party subcontracting or assigning this MOU must monitor, evaluate and account for the subcontractor(s)/assignee's services and operations. Any assignment of this MOU or subcontract entered into in violation of this provision by either party will be void.

**6. INDEPENDENT CONTRACTOR STATUS**

In the performance of the services under this MOU, the parties shall be, and acknowledge that they are in fact and law, independent contractors and not an agent or employee of the other party.

**7. WAIVER**

The waiver of any breach in the terms hereof, or of any default hereunder, is not deemed a waiver of any subsequent breach or default, whether of the same or similar nature, and does not affect the terms hereof. No waiver or modification is valid or binding unless in writing and signed by both parties.

**8. SEVERABILITY OF PROVISIONS**

If any provisions of this MOU are held invalid, the remainder of this MOU remains in force and effect.

**9. AMENDMENTS**

Any adjustment to this MOU shall be effective only upon the parties' mutual execution of an amendment in writing.

**10. PRIVACY AND SECURITY PROVISIONS**

District shall comply with the information privacy and security provisions contained in Exhibit A, attached to and incorporated into this MOU.

## **11. INSURANCE**

During the term of this M.O.U., LEA shall provide to HHSA, and HHSA shall provide to LEA, a current certificate of policy evidencing its comprehensive and general liability insurance coverage in a sum not less than \$2,000,000 aggregate and \$1,000,000 per occurrence. LEA shall also provide HHSA and HHSA shall also provide LEA, with a written endorsement naming the other party as an additional insured, and such endorsement shall also state "Such insurance as afforded by this policy shall be primary, and any insurance carried by LEA or HHSA shall be excess and noncontributory." Any and all insurance coverage may be provided by a Joint Powers Authority or other Self-Insurance program. Coverage shall provide notice to the additional insured of any change in or limitation of coverage or cancellation of the policy no less than thirty (30) days prior to the effective date of the change, limitation or cancellation.

## **12. NOTICES**

Communications relating to this MOU will be in writing, and shall be delivered personally, sent by United States mail, first class postage prepaid, or by private messenger or courier service to the addresses set forth below:

Yolo County Health and Human Services Agency	Karen Larsen, Director 137 N. Cottonwood Street XXXXXX, CA 95695
---	--

Davis Joint Unified School District	Bruce E. Colby Chief Business & Operations Officer 526 B Street Davis, CA 95616
--	--

The parties agree to comply with the terms and conditions contained in this MOU.

//

//

//

//

// [Signatures on the next page]

IN WITNESS WHEREOF, the parties have executed this MOU.

**DAVIS JOINT UNIFIED SCHOOL DISTRICT**

\_\_\_\_\_  
By: Bruce E. Colby, Chief Business & Operations Officer

Date: \_\_\_\_\_

**COUNTY OF YOLO,**  
for the benefit of the Health and Human Services Agency

\_\_\_\_\_  
By: Karen Larsen, Director

Date: \_\_\_\_\_

Approved as to Form:  
Philip J. Pogledich, County Counsel

\_\_\_\_\_  
By: Carrie Scarlata, Assistant County Counsel

Date: \_\_\_\_\_

## **EXHIBIT A**

### **ARTICLE 14: INFORMATION PRIVACY AND SECURITY PROVISIONS**

A. This Article is intended to protect the privacy and security of specified County information that District may receive, access, or transmit, under this MOU. 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 MOU between the County and District with regards to protection of PI and PII. This includes the IEA and the CMPPA to the extent the District 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 Yolo ("County") wishes to disclose to District 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, District, 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 District 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 District prior to the disclosure of PHI to District, 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 District.

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 District, 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 District 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 District.

14.1.3.1 Permitted Uses and Disclosures of County PHI by District. District 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, District 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, District 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 District 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 District 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 District 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 District 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 District's operations and the nature and scope of its activities.

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

14.1.3.6 District's Agents and Subcontractors. District shall ensure that any agent, including a subcontractor, to whom it provides County PHI, imposes the same conditions on such agents that apply to District 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. District 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 District.

14.1.3.6.1 In accordance with section 164.504(e) (1) (ii), upon District's knowledge of a material breach or violation by its subcontractor of the agreement between District and the subcontractor, District 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. District 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 District 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 District shall make internal practices, books, and records relating to the use and disclosure of District PHI received from, or created or received by District 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. District 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. District shall make any required amendment(s) to County PHI that were requested by an Individual, in accordance with HIPAA. District 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. District 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 District maintains electronic health records as of January 2009, District shall provide an accounting of disclosures including those for Treatment, Payment, and Healthcare Operations (TPO), effective January 2014. If District acquires electronic health records for County after January 1, 2009, District 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. District 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. District shall provide Individuals access and copies of their County PHI, as required by HIPAA, to include:

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

14.1.3.10 Reporting of Unauthorized Use or Disclosure. District 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 District 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 District 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 District 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 District 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 District.

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, District 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. District shall immediately investigate such security incident, breach, or unauthorized access, use or disclosure of County PHI. Within seventy-two (72) hours of the discovery, District shall submit an updated report to the County.

14.1.3.10.5 Complete Report. District 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 formally to the County in writing 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, District 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 District or its subcontractors, agents or vendors, District 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 are 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 are 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.

### **14.3 DATA SECURITY REQUIREMENTS**

District 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. District 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 District 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. District shall retain each workforce member's District background check documentation for a period of three (3) years following contract termination.

14.3.1.2 Complete privacy and security training, at District'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. District 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. District 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 District facilities where District workers use or disclose County PHI and/or County PII/PI. District 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 District functions in one building in work areas that are not securely segregated. District 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. District 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 and password secured. 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.

14.3.3.2 Have critical security patches applied, with system reboot if necessary. 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.)

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 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. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

14.3.3.10 All data transmissions of County PHI and/or County PII/PI outside the secure internal network shall be encrypted. 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.

14.3.5 Paper Document Controls. District 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 District 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 HHS Privacy Officer to use another method is obtained.

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