AGENDA ITEM NO.
C-9

COUNTY OF HUMBOLDT

For the meeting of: March 21, 2017

Date: February 16, 2017

To: Board of Supervisors

From: Connie Beck, Director CB
Department of Health and Human Services

Subject: Medi-Cal Data Privacy and Security Agreement with the California Department of Social Services

RECOMMENDATION(S):
That the Board of Supervisors:

1. Approve the attached Medi-Cal Data Privacy and Security Agreement with the California Department of Social Services (CDSS);

2. Authorize the Department of Health and Humans Services (DHSS)-Social Services Director to sign the agreement and any subsequent amendments or other documents related to this agreement; and

3. Direct the Clerk of the Board to forward one (1) certified copy of the board report to the DHHS-Social Services Attn: Sharon Wolff.

SOURCE OF FUNDING:

Social Services Fund

DISCUSSION:

Prepared by Sharon Wolff, Staff Services Analyst II CAO Approval

REVIEW:
Auditor County Counsel Human Resources Other

TYPE OF ITEM:
X Consent
_____ Departmental
_____ Public Hearing
_____ Other _____

PREVIOUS ACTION/REFERRAL:

Board Order No. C-10

Meeting of: 8/23/16

BOARD OF SUPERVISORS, COUNTY OF HUMBOLDT
Upon motion of Supervisor Fennell Seconded by Supervisor Sundberg

Ayes Sundberg, Fennell, Bass, Wilson
Nays
Abstain
Absent Bohn

and carried by those members present, the Board hereby approves the recommended action contained in this Board report.

Dated: Mar 21, 2017
By:
Kathy Hayes, Clerk of the Board

On August 23, 2016, the Board approved (item C-10) the Medi-Cal Data Privacy and Security Agreement between DHHS-Social Services and the California Department of Health Care Services (CDHCS). The agreement before the Board today is substantially similar. CDSS issued an All County Letter (ACL 16-100) on January 12, 2017 which put forth the requirement for individual county agreements in order to meet the personally identifiable information (PII) data protection requirements of the Social Security Administration (SSA).

DHHS-Social Services staff utilize the Medi-Cal Eligibility Data System (MEDS) and Income and Eligibility Verification System (IEVS) to access PII and eligibility data in order to administer multiple programs including CalFresh, CalWORKs, Foster Care and General Relief. The privacy and security agreement covers DHHS-Social Services workers who assist in the administration of the various eligibility programs, and who access, use and disclose PII. PII consists of any information used to identify an individual, including a person's name, social security number, date of birth, driver's license number, or identification number.

Under the terms of this agreement, DHHS-Social Services staff may use or disclose this information only to perform functions, activities or services directly related to the administration of the specific eligibility programs. Additionally, DHHS staff will be trained on the requirements of the agreement to safeguard PII. DHHS-Social Services will train all new staff within 30 days of employment and will provide ongoing reminders on the privacy and security requirements. DHHS-Social Services has established and will maintain ongoing oversight for monitoring workforce compliance. DHHS-Social Services also agrees to ensure that all PII is physically safe from access by unauthorized persons and will comply with the computer security safeguards outlined in the agreement.

It should be noted that two of the attachments to the agreement are considered highly confidential and therefore cannot be disclosed in an open session of the Board. These documents are the Computer Matching and Privacy Protection Act agreement between the Social Security Administration (SSA) and DHHS as well as the Computer Matching agreement between the Department of Homeland Security, Citizenship and Immigration Services and CDHCS. The documents are not consequential to the agreement before the Board today. These agreements include highly sensitive and confidential information and are not public records.

At this time, DHHS-Social Services recommends the Board approve this agreement and authorize the DHHS-Social Services Director to sign the agreement and any subsequent amendments or other documents related to this agreement.

FINANCIAL IMPACT:

DHHS-Social Services has made all hardware and software upgrades necessary to comply with the previous agreement. The costs of maintaining and operating the security safeguards associated with this agreement have been budgeted in the approved fiscal year 2016-17 Budget, in Fund 1160, Budget Unit 511 in the amount of $250,000. There will be no impact to the county's General Fund.

This agreement supports the Board's Strategic Framework by enforcing laws and regulations to protect residents and by creating opportunities for improved safety and health.

OTHER AGENCY INVOLVEMENT:

None

ALTERNATIVES TO STAFF RECOMMENDATIONS:

The Board of Supervisors can choose not to approve the agreement. This is not recommended because the United States SSA requires that CDSS enters into these agreements with all California county Health & Human Services Departments in order for the department to continue accessing PII data for the administration of public benefit programs.

ATTACHMENTS:

Attachment 1: Agreement with CDSS for Medi-Cal Data Privacy and Security

STATE OF CALIFORNIA—HEALTH AND HUMAN SERVICES AGENCY
DEPARTMENT OF SOCIAL SERVICES
744 P Street • Sacramento, CA 95814 • *www.cdss.ca.gov*

CDSS
WILL LIGHTBOURNE
DIRECTOR

EDMUND G. BROWN JR.
GOVERNOR

REASON FOR THIS TRANSMITTAL
[ ] State Law Change
[ ] Federal Law or Regulation Change
[ ] Court Order
[ ] Clarification Requested by One or More Counties
[X] Initiated by CDSS

January 12, 2017

ALL COUNTY LETTER (ACL) NO. 16-100

TO: ALL COUNTY WELFARE DIRECTORS

SUBJECT: CDSS PRIVACY AND SECURITY AGREEMENT

The purpose of this All County Letter (ACL) is to notify counties of the California Department of Social Services (CDSS) Privacy and Security Agreement (PSA) and to provide counties with instructions for returning signed agreements to CDSS within 90 days of this ACL. The purpose of the PSA between CDSS and each county department is to ensure the security and privacy of Personally Identifiable Information (PII) contained in the Medi-Cal Eligibility Data System (MEDS), the Applicant Income and Eligibility Verification System (IEVS), and in data received from the Social Security Administration (SSA) and other sources. Because counties have access to the SSA-provided information, the SSA requires that CDSS enter into individual agreements with counties to safeguard this information. The terms of this PSA are similar to those of the Department of Health Care Services (DHCS) PSA.

All counties must return signed PSAs in order to ensure the continued transmission of SSA, MEDS, and IEVS PII data to the counties as part of administration of the public social services programs described in the agreements. Please note that each county department that utilizes SSA, MEDS, and IEVS PII data to administer CDSS programs must return a signed PSA.

INCORPORATED EXHIBITS

The incorporated exhibits are highly sensitive and confidential. Only the County Privacy and Information Security Officers may receive these documents. All disclosure shall be limited to the appropriate parties or individuals responsible for and involved with decision making for the safeguarding of SSA, MEDS, and IEVS PII data. These documents are not public and shall not be published on any website accessible by or otherwise made available to the public. County Privacy and/or Information Security Officers who wish to receive the following CDSS PSA Exhibits must submit requests via email to the CDSS Information Security Office PSA email box at cdsspsa@dss.ca.gov.

Exhibit A:

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency (05/25/2016)
- Information Exchange Agreement between SSA and CDSS (IEA-F 10/30/2014 and IEA-S 10/30/2014)
- The SSA Technical System Security Requirements (TSSR), also known as the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies exchanging electronic information with the SSA (version 7.0, 7/2015)

Exhibit B:

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and California Department of Social Services (CA-DSS) (12/15/2015)

SUBMISSION GUIDELINES

Counties should follow the instructions below when returning signed PSAs to CDSS. The county department should not modify any of the PSA language, except as instructed below.

- The county must complete the Preamble of the PSA by entering the name of the county and the county department.
- The county must complete the Preamble of the PSA by designating the applicable programs.
- The county must complete Section XX of the PSA by entering signatory information. The name and title of the signatory must be printed or typed.

Within 90 days of this ACL, please send CDSS two copies of the completed and signed PSAs per county department using the data, both of which are to contain the original signature of the county department authorized official. Once obtained, the PSAs will be executed by CDSS and returned to each respective county department.

When transmitting the PSAs to CDSS, counties must include a contact name, telephone number, email address and physical mailing address to be used when CDSS returns the signed PSAs, and as needed for other communication purposes.

Counties that are unable to return the signed PSAs within 90 days of the date of this ACL should respond to the email address below with the following information:

- Date signed PSAs will be returned; and/or
- If additional time will be needed to implement the compliance requirements of the PSA, the expected date of implementation; and/or
- Reason(s) why the county department will be unable to implement the compliance requirements of the PSA

Agreements must be returned to the following address:

California Department of Social Services
Information Security Office
744 P Street, MS 9-9-70
Sacramento, CA 95814

In the event that there are any questions or concerns regarding any of the information in this letter or implementing the requirements of the PSA, please contact the Information Security Office PSA email box at cdsspsa@dss.ca.gov.

Sincerely,

Original Document Signed By:

PETE CERVINKA
Chief Deputy Director
California Department of Social Services

Attachment

c: CWDA

PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Social Services and the

County of Humboldt **, Department of** Social Services

PREAMBLE

The California Department of Social Services (CDSS) and the County of Humboldt, Department of Social Serv. (County Department) enter into this Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Social Security Administration (SSA), Medi-Cal Eligibility Data System (MEDS) and Applicant Income and Eligibility Verification System (IEVS) Personally Identifiable Information (PII), covered by this Agreement and referred to hereinafter as PII, that the counties access through CDSS and the Department of Health Care Services (DHCS). This Agreement covers the following twelve (12) programs; please check the applicable box(s) for your County Department:

☑ CalFresh;

☑ California Food Assistance Program (CFAP);

☑ California Work Opportunity and Responsibility to Kids Program (CalWORKs);

☑ Cash Assistance Program for Immigrants (CAPI);

☑ Entrant Cash Assistance (ECA);

☑ Foster Care (FC) (eligibility);

☑ Kinship Guardianship Assistance Program (Kin-GAP) (eligibility);

☑ Federal Guardianship Assistance Program (Fed-GAP) (eligibility);

☑ General Assistance/General Relief (GA/GR);

☑ Refugee Cash Assistance (RCA); and

☑ Trafficking and Crime Victims Assistance Program (TCVAP).

The CDSS has an Inter-Agency Agreement (IAA) with DHCS that allows CDSS and local county agencies to access SSA and MEDS data for the purpose of determining eligibility for the programs listed above. The IAA requires that CDSS may only share SSA and MEDS data if its contract with the entity with whom it intends to share the data reflects the entity's obligations under the IAA.

The County Department in its administration of the social services programs utilizes SSA and MEDS data in conjuction with other system data, for eligibility determinations.

This Agreement covers the County of Humboldt, Department of Social Services and its staff (county staff), who access, use, or disclose PII covered by this Agreement, to assist in the administration of programs.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. "**Assist in the Administration of the Program**" means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.
2. "**Breach**" refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
3. "**County staff**" means those county employees, contractors, subcontractors, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.
4. "**PII**" is personally identifiable information that is obtained through the MEDS or IEVS on behalf of the programs and can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. The PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded.
5. "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.

6. "**Secure Areas**" means any area where:
   a. County staff assist in the administration of their program;
   b. County staff use or disclose PII; or
   c. PII is stored in paper or electronic format.

MEMORANDUM OF UNDERSTANDING

NOW THEREFORE, CDSS and County Department mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. The County Department staff covered by this Agreement (county staff) may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et.seq and Welfare and Institutions Code section 10850 **(County Department please insert alternative statute that authorizes the use of data if 10850 is inapplicable)** or as authorized or required by law. Disclosures, which are authorized or required by law, such as a court order, or are made with the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by CDSS. No county staff shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

B. Pursuant to this Agreement, county staff may only use PII to perform administrative functions related to administering their respective programs.

C. Access to PII shall be restricted to county staff who need to perform their official duties to assist in the administration of their respective programs.

D. County staff who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

The County Department agrees to advise county staff who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department shall implement the following personnel controls:

A. ***Employee Training.*** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by county staff, including, but not limited to:

   1. Provide initial privacy and security awareness training to each new county staff within thirty (30) days of employment and;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all county staff. Three (3) or more security reminders per year are recommended;
3. Maintain records indicating each county staff's name and the date on which the privacy and security awareness training was completed;
4. Retain training records for a period of three (3) years after completion of the training.

B. ***Employee Discipline***.

1. Provide documented sanction policies and procedures for county staff who fail to comply with privacy policies and procedures or any provisions of these requirements.
2. Sanction policies and procedures shall include termination of employment when appropriate.

C. ***Confidentiality Statement***. Ensure that all county staff sign a confidentiality statement. The statement shall be signed by county staff prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years.

The statement shall include at a minimum:

1. General Use;
2. Security and Privacy Safeguards;
3. Unacceptable Use; and
4. Enforcement Policies.

D. ***Background Screening***.

1. Conduct a background screening of a county staff before they may access PII.
2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls;
3. The County Department shall retain each county staff's background screening documentation for a period of three (3) years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

To ensure compliance with the privacy and security safeguards in this Agreement the County Department shall perform the following:

A. Conduct periodic privacy and security reviews of work activity by county staff, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.

B. The periodic privacy and security reviews must be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of their program, and the use or disclosure of PII.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

B. Assign county staff to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

The County Department shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The County Department agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of the County Department facilities where county staff assist in the administration of their program and use, disclose, or store PII.

B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:

   1. Properly coded key cards
   2. Authorized door keys
   3. Official identification

C. Issue identification badges to county staff.

D. Require county staff to wear these badges where PII is used, disclosed, or stored.

E. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

F. Ensure there are security guards or a monitored alarm system at all times at the County Department facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.

G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized county staff. Visitors to the data center area must be escorted at all times by authorized county staff.

H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County Department and non-County Department functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

I. The County Department shall have policies that include, based on applicable risk factors, a description of the circumstances under which the county staff can transport PII, as well as the physical security requirements during transport. A County Department that chooses to permit its county staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

J. The County Department shall have policies that indicate county staff are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

K. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

VI. TECHNICAL SECURITY CONTROLS

A. ***Workstation/Laptop Encryption.*** All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

B. ***Server Security***. Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

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

D. ***Mobile Device and Removable Media***. All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

E. ***Antivirus Software***. All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

F. ***Patch Management***.

1. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
2. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
3. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

G. ***User IDs and Password Controls***.

1. All users must be issued a unique user name for accessing PII.
2. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty-four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
3. Passwords are not to be shared.

4. Passwords must be at least eight (8) characters.
5. Passwords must be a non-dictionary word.
6. Passwords must not be stored in readable format on the computer or server.
7. Passwords must be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less.
8. Passwords must be changed if revealed or compromised.
9. Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
    a. Upper case letters (A-Z)
    b. Lower case letters (a-z)
    c. Arabic numerals (0-9)
    d. Special characters (!,@,#, etc.)

H. ***User Access***. In conjunction with CDSS and DHCS, County Department management should exercise control and oversight over the authorization of individual user access to SSA data, MEDS, IEVS, and over the process of issuing and maintaining access control numbers, IDs, and passwords.

I. ***Data Destruction***. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

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

K. ***Warning Banners***. The systems providing access to PII must display a warning banner stating, at a minimum:

1. Data is confidential;
2. Systems are logged;
3. System use is for business purposes only, by authorized users; and
4. Users shall log off the system immediately if they do not agree with these requirements.

L. ***System Logging***.

1. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.

2. The audit trail shall:
    a. Be date and time stamped;
    b. Log both successful and failed accesses;
    c. Be read-access only; and
    d. Be restricted to authorized users.
3. If PII is stored in a database, database logging functionality shall be enabled.
4. Audit trail data shall be archived for at least three (3) years from the occurrence.

M. ***Access Controls***. The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

N. ***Transmission Encryption***.

1. All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.
2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

O. ***Intrusion Prevention***. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. ***System Security Review***.

1. The County Department must ensure audit control mechanisms are in place.
2. All systems processing and/or storing PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
3. Reviews should include vulnerability scanning tools.

B. ***Log Reviews***. All systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

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

D. ***Anomalies***. When the County Department or DHCS suspects MEDS usage anomalies, the County Department will work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to CDSS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. ***Emergency Mode Operation Plan***. The County Department must establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format 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. It is recommended that County Department conduct periodic disaster recovery testing, including connectivity exercises conducted with DHCS and CDSS, if requested.

B. ***Data Centers***. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

C. ***Data Backup and Recovery Plan***.

1. The County Department shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
2. The documented backup procedures shall contain a schedule which includes incremental and full backups.
3. The procedures shall include storing backups offsite.
4. The procedures shall ensure an inventory of backup media.
5. The County Department shall have established documented procedures to recover PII data.
6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
7. It is recommended that the County Department periodically test the data recovery process.

IX. PAPER DOCUMENT CONTROLS

A. ***Supervision of Data.*** The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles.*** The County Department shall have policies that include, based on applicable risk factors, a description of the circumstances under which the county staff can transport PII, as well as the physical security requirements during transport. A County Department that chooses to permit its county staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

C. ***Public Modes of Transportation.*** The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

D. ***Escorting Visitors.*** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

E. ***Confidential Destruction.*** PII must be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data.*** The PII must not be removed from the premises of County Department except for identified routine business purposes or with express written permission of CDSS.

G. ***Faxing.***

1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. ***Mailing.***

1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the County Department obtains prior written permission from CDSS to use another method.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the County Department agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

A. ***Initial Notice to DHCS***:

The County Department will provide initial notice to DHCS with a copy to CDSS. The DHCS is acting on behalf of CDSS, for purposes of receiving reports of privacy and information security incidents and breaches. The County Department agrees to perform the following incident reporting to DHCS.

Immediately upon discovery of a suspected security incident that involves data provided to DHCS by the SSA, the County Department shall notify DHCS by email or telephone.

Within one working day of discovery, the County Department shall notify DHCS by email or telephone of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notice shall be made using the "DHCS Privacy Incident Report" (PIR) form, including all information known at the time. The County Department shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, select "Privacy & HIPAA" and then "County Use") or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx. Initial, Investigation, and Completed PIRs are submitted to the DHCS Privacy Office and the DHCS Information Security Office. When using this form to report PII incidents, the County Department shall also include in the report the system(s) and program(s) involved as known at the time of reporting.

A breach shall be treated as discovered by the County Department as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the County Department. Notice shall be provided to the DHCS Privacy Office and the DHCS Information Security Office.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the County Department shall take:

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

B. ***Investigation and Investigative Report.*** The County Department shall immediately investigate breaches and security incidents involving PII, and, if the initial PIR did not include all of the information marked with an asterisk, or if new or updated information is available, submit an updated PIR **within seventy-two (72) hours of the discovery**. The updated PIR shall include all of the information marked with an asterisk, and all other applicable information listed on the form, to the extent known at that time.

C. ***Complete Report.*** If all of the required information was not included in either the initial report, or the investigation report, then a separate complete report must be submitted **within ten (10) working days of the discovery**. The Complete Report of the investigation shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of SSA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Health Insurance Portability and Accountability Act (HIPAA) regulations, and/or state law. The report shall also include a full, detailed corrective action plan (CAP), including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDSS or DHCS requests information in addition to that listed on the PIR, the County Department shall make reasonable efforts to provide such information. The DHCS will review the County Department's determination of whether a breach occurred, whether individual notifications are required, and the CAP, and will make recommendations to CDSS. The CDSS will make the final breach and CAP determinations. If necessary, an updated PIR may be used to submit revised or additional information after the Completed Report is submitted.

D. ***Notification of Individuals.*** When applicable state or federal law requires a breaching entity to notify individuals of a breach or unauthorized disclosure of their PII, the following provisions apply: If the cause of the breach is attributable to the County Department or its subcontractors, agents or vendors, the County Department shall pay any costs of such notifications, as well as any and all costs associated with the breach. The notifications shall comply with the requirements set forth in California Civil Code section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days. The CDSS shall review the time, manner and content of any such notifications; CDSS may elect to assign responsibility for such notification to the County Department. In the event CDSS assigns notification responsibility to the County Department, CDSS shall provide the County Department with the appropriate direction and procedures to ensure notice is provided pursuant to applicable law. If the cause of the breach is attributable to CDSS, CDSS shall pay any costs associated with such notifications. If there is any question as to whether CDSS or the County Department is responsible for the breach, CDSS and the County Department shall jointly determine responsibility for purposes of allocating the costs of such notices.

E. ***Responsibility for Reporting of Breaches when Required by State or Federal Law***. If the cause of a breach is attributable to the County Department or its agents, subcontractors or vendors, the County Department is responsible for reporting the breach and all costs associated with the breach. If the cause of the breach is attributable to CDSS, CDSS is responsible for reporting the breach and for all costs associated with the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS (if the breach involves MEDS or SSA data), CDSS, and the County Department shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

F. ***CDSS and DHCS Contact Information***. To direct communications to the above referenced CDSS and DHCS staff, the County Department shall initiate contact as indicated herein. The CDSS and DHCS reserves the right to make changes to the contact information below by giving written notice to the County Department. Said changes shall not require an amendment to this Agreement to which it is incorporated.

CDSS Information Security & Privacy Office	**DHCS Privacy Office**
California Department of Social Services Information Security & Privacy Office 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558	DHCS Privacy Office Office of HIPAA Compliance MS 4722 P.O. Box 997413 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 or (866) 866-0602

XI. COMPLIANCE WITH SSA AGREEMENT

The County Department agrees to comply with substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between SSA and CDSS, known as the Information Exchange Agreement (IEA), which are appended and hereby incorporated in to this Agreement (Exhibit A). The specific sections of the IEA with substantive privacy and security requirements, which are to be complied with by the County Department are in the following sections:

- Section E, Security Procedures;
- Section F, Contractor/Agent Responsibilities;
- Section G, Safeguarding and Reporting Responsibilities for PII; and
- Attachment 4, Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR).

If there is any conflict between a privacy and security standard in these sections of the IEA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If SSA changes the terms of its agreement(s) with CDSS, as soon as reasonably possible after receipt, CDSS will supply copies to the County Welfare Directors Association (CWDA). CDSS will also propose a target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, CDSS will supply copies of the changed agreement to the CWDA and the counties, along with the compliance date expected by SSA. If a County Department is not able to meet the SSA compliance date, it must submit a CAP to CDSS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential County Department resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

XII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County Department agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS, which is appended and hereby incorporated into this Agreement (Exhibit B). If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If DHS-USCIS changes the terms of its agreement(s) with CDSS, CDSS will, as soon as reasonably possible after receipt, supply copies to CWDA as well as the CDSS proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once a target date for compliance is determined by DHS-USCIS, CDSS will supply copies of the changed agreement to the CWDA and the County Department, along with the compliance date expected by DHS-USCIS. If a County Department is not able to meet the DHS-USCIS compliance date, it must submit a CAP to CDSS for review and approval at least thirty (30) days prior to the DHS-USCIS compliance date. Any potential County Department resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

XIII. COUNTY DEPARTMENT'S AGENTS AND SUBCONTRACTORS

The County Department agrees to enter into written agreements with any agents, including subcontractors and vendors, to whom County Department provides PII received from or created or received by County Department in performing functions or activities related to the administration of their program that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to the County Department with respect to PII, including restrictions on disclosure of PII and the use of appropriate administrative, physical, and technical safeguards to protect such PII. The County Department shall incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the County Department.

XIV. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the County Department agrees to allow CDSS or DHCS (on behalf of CDSS) to inspect the facilities, systems, books, and records of the County Department, with reasonable notice from CDSS or DHCS, in order to perform assessments and reviews. Such inspections shall be scheduled at times that take into account the operational and staffing demands. The County Department agrees to promptly remedy any violation of any provision of this Agreement and certify the same to CDSS in writing, or to enter into a written CAP with CDSS containing deadlines for achieving compliance with specific provisions of this Agreement.

XV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

In the event of litigation or administrative proceedings involving CDSS based upon claimed violations by the County Department of the privacy or security of PII, or federal or state laws or agreements concerning privacy or security of PII, the County Department shall make all reasonable effort to make itself and county staff assisting in the administration of their program and using or disclosing PII available to CDSS at no cost to CDSS to testify as witnesses. The CDSS shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to the County Department at no cost to the County Department to testify as witnesses, in the event of litigation or administrative proceedings involving the County Department based upon claimed violations by CDSS of the privacy or security of PII, or state or federal laws or agreements concerning privacy or security of PII.

XVI. AMENDMENT OF AGREEMENT

The CDSS and the County Department acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that an amendment to this Agreement may be required to ensure compliance with all data security and privacy procedures. Upon request by CDSS, the County Department agrees to promptly enter into negotiations concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. The CDSS may terminate this Agreement upon thirty (30) days written notice if the County Department does not promptly enter into negotiations to amend this Agreement when requested to do so, or does not enter into an amendment that CDSS deems necessary.

Each amendment shall be properly identified as Agreement No., Amendment No. (A-1, A-2, A-3, etc.) to identify the applicable changes to this Agreement, and be effective upon execution by the parties.

XVII. TERM OF AGREEMENT

The term of this agreement shall be upon signature and approval of CDSS through October 1, 2019.

XVIII. TERMINATION

A. This Agreement shall terminate on October 1, 2019, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement through a formal amendment. County Department requests for an extension must be justified and approved by CDSS and limited to no more than a six-month extension. Such an extension may, upon County Department request and CDSS approval, be renewed for one additional six-month period. No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties, and approved as required. No oral understanding or agreement not incorporated in the Agreement is binding upon any of the parties.

B. ***Survival:*** All provisions of this Agreement that provide restrictions on disclosures of PII and that provide administrative, technical, and physical safeguards for the PII in the County Department's possession shall continue in effect beyond the termination of the Agreement, and shall continue until the PII is destroyed or returned to CDSS.

XIX. TERMINATION FOR CAUSE

Upon CDSS' knowledge of a material breach or violation of this Agreement by the County Department, CDSS may provide an opportunity for the County Department to cure the breach or end the violation and may terminate this Agreement if the County Department does not cure the breach or end the violation within the time specified by CDSS. This Agreement may be terminated immediately by CDSS if the County Department has breached a material term and CDSS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department must destroy all PII in accordance with Section VI, above. The provisions of this Agreement governing the privacy and security of the PII shall remain in effect until all PII is destroyed and CDSS receives a certificate of destruction.

XX. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on the day the final signature is obtained.

For the County of_____ Department of _____,

_____	_____
(Signature)	(Date)
_____	_____
(Name – Print or Type)	(Title – Print or Type)

For the California Department of Social Services,

_____	_____
(Signature)	(Date)
Deborah Pearce	Chief, Contracts & Purchasing Bureau
(Name)	(Title)

EXHIBIT A

These are sensitive documents that are provided separately upon request to the County's Privacy and/or Information Security Officer.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency (5/25/2016)
- Information Exchange Agreement between SSA and CDSS (IEA-F 10/30/2014 and IEA-S 10/30/2014)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR) (version 7.0, 7/2014)

EXHIBIT B

These are sensitive documents that are provided separately upon request to the County's Privacy and/or Information Security Officer.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and California Department of Social Services (CA-DSS) (12/15/2015)