2019 PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Social Services and the

County of San Bernardino ,

Department/Agency of Human Services Group

PREAMBLE

The California Department of Social Services (CDSS) and the

County of San Bernardino ,

Department/Agency of Human Services Group

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 programs:

- 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)/Refugee Cash Assistance (RCA);
- Foster Care (FC) (eligibility);
- Kinship Guardianship Assistance Program (Kin-GAP) (eligibility);
- Federal Guardianship Assistance Program (Fed-GAP) (eligibility);
- General Assistance/General Relief (GA/GR); 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 in order to Assist in the Administration of the Program 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/Agency utilizes SSA and MEDS data in conjunction with other system data in order to Assist in the Administration of the Program for the programs listed above.

This Agreement covers the

County of San Bernardino ,

Department/Agency of Human Services Group

and its staff (County Workers), 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 Worker**" 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 directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of the programs, which can be used alone, or in conjunction with any other reasonably available information to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including, but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

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 Workers assist in the administration of their program;

   b. County Workers use or disclose PII; or

   c. PII is stored in paper or electronic format.

7. "**SSA-provided or verified data (SSA data)**" means:

   a. Any information under the control of the Social Security Administration (SSA) provided to CDSS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or;

   b. Any information provided to CDSS, including a source other than SSA, but in which CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

   For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

AGREEMENTS

CDSS and County Department/Agency mutually agree as follows:

I.   PRIVACY AND CONFIDENTIALITY

A. County Workers 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 or as authorized or required by law. Disclosures required by law or that are made with the explicit written authorization of the client are allowable. Any other use or disclosure of PII requires the express approval in writing of CDSS. No County Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

B. Pursuant to this Agreement, County Workers may only use PII to assist in administering their respective programs.

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

D. County Workers 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/Agency agrees to advise County Workers 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/Agency 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 Workers, including, but not limited to:

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

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three (3) or more security reminders per year are recommended;

3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed; and

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 Workers 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 Workers sign a confidentiality statement. The statement shall be signed by County Workers 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, or five (5) years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

The statement shall include, at a minimum, a description of the following:

1. General Use of the PII;

2. Security and Privacy Safeguards for the PII;

3. Unacceptable Use of the PII; and

4. Enforcement Policies.

D. ***Background Screening***.

1. Conduct a background screening of a County Worker 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/Agency shall retain each County Worker's background screening documentation for a period of three (3) years following conclusion of employment relationship.

III.   <u>MANAGEMENT OVERSIGHT AND MONITORING</u>

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

A. Conduct periodic privacy and security reviews of work activity by County Workers, 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 shall 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.   <u>INFORMATION SECURITY AND PRIVACY STAFFING</u>

The County Department/Agency 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. Provide CDSS with applicable contact information for these designated individuals by emailing CDSS at cdsspsa@dss.ca.gov. Any changes to this information should be reported to CDSS within ten (10) days.

C. Assign County Workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V.   <u>PHYSICAL SECURITY</u>

The County Department/Agency 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/Agency agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of the County Department/Agency facilities where County Workers 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 Workers.

D. Require County Workers 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/Agency 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 Workers. Visitors to the data center area shall be escorted at all times by authorized County Workers.

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

J. The County Department/Agency shall have policies that indicate County Workers are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., inclusive of 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. <u>TECHNICAL SECURITY CONTROLS</u>

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

B. ***Server Security***. Servers containing unencrypted PII shall 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, shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption shall 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, shall 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, shall have critical security patches applied, with system reboot if necessary.

2. There shall 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 shall 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, shall have compensatory controls implemented to minimize risk.

G. *User IDs and Password Controls*.

1. All users shall be issued a unique user name for accessing PII.

2. Username shall be promptly disabled, deleted, or the password changed within, at most, twenty-four (24) hours of the transfer or termination of an employee. Note: Twenty-four (24) hours is defined as one (1) working day.

3. Passwords are not to be shared.

4. Passwords shall be at least eight (8) characters.

5. Passwords shall be a non-dictionary word.

6. Passwords shall not be stored in readable format on the computer or server.

7. Passwords shall be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less. Non-expiring passwords are permitted when in full compliance with NIST SP 800-63B Authenticator Assurance Level (AAL) 2.

8. Passwords shall be changed if revealed or compromised.

9. Passwords shall be composed of characters from at least three (3) of the four (4) of the following 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/Agency management should exercise control and oversight over the authorization of individual user access to SSA data via, 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 shall 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 shall 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 shall 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 that provide access to PII shall 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 of the audit trail.

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 shall 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, shall be protected by an intrusion detection and prevention solution.

VII. <u>AUDIT CONTROLS</u>

A. **System Security Review**.

1. The County Department/Agency shall ensure audit control mechanisms are in place.

2. All systems processing and/or storing PII shall 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 shall 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 shall 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/Agency or DHCS suspects MEDS usage anomalies, the County Department/Agency 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/Agency shall 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/Agency 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, shall include environmental protection such as cooling, power, and fire prevention, detection, and suppression; and appropriate protection from other threats, including but not limited to flood, earthquake, and terrorism.

C. *Data Backup and Recovery Plan*.

1. The County Department/Agency 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 containing PII offsite.

4. The procedures shall ensure an inventory of backup media.

5. The County Department/Agency 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/Agency 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/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII to 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., inclusive of 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 shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. *Removal of Data*. The PII shall not be removed from the premises of County Department/Agency 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/Agency 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/Agency 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/Agency will provide initial notice to DHCS by email, or alternatively, by telephone if email is unavailable, of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII 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/Agency agrees to perform the following incident reporting to DHCS:

   1. If a suspected security incident involves PII provided or verified by SSA, the County Department/Agency shall immediately notify DHCS upon discovery. For more information on SSA data, please see the Definition section of this Agreement.

2. If a suspected security incident does not involve PII provided or verified by SSA, the County Department/Agency shall notify DHCS within one (1) working day of discovery.

If it is unclear if the security incident involves SSA data, the County Department/Agency shall immediately report the incident upon discovery.

A County Department/Agency shall notify DHCS of all personal information, as defined by California Civil Code Section 1798.3(a), that may have been accessed, used, or disclosed in any suspected security incident or breach, including but not limited to case numbers.

Notice shall be made using the DHCS Privacy Incident Report (PIR) form, including all information known at the time. The County Department/Agency shall use the most current version of this form, which is available on the DHCS Privacy Office website at:
http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx.
All PIRs and supporting documentation are to be submitted to DHCS via email using the "DHCS Breach and Security Incidents Reporting" contact information found below in Subsection F.

A breach shall be treated as discovered by the County Department/Agency 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/Agency.

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

1. Prompt action to mitigate any risks or damages involved with the occurrence and to protect the operating environment; and

2. Any action pertaining to such occurrence required by applicable Federal and State laws and regulations.

B. Investigation and Investigative Report. The County Department/Agency shall immediately investigate breaches and security incidents involving PII. If the initial PIR was submitted incomplete and if new or updated information is available, submit an updated PIR to DHCS within seventy-two (72) hours of the discovery. The updated PIR shall include any other applicable information related to the breach or security incident known at that time.

C. ***Complete*** Report. If all of the required information was not included in either the initial report or the investigation PIR submission, then a separate complete report shall be submitted within ten working days of the discovery. The Complete Report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law. The report shall also include a Corrective Action Plan (CAP) that shall include, at minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If DHCS requests additional information related to the incident, the County Department/Agency shall make reasonable efforts to provide DHCS with such information. If necessary, the County Department/Agency shall submit an updated PIR with revisions and/or additional information after the Completed Report has been provided. DHCS will review and determine whether a breach occurred and whether individual notification is required. DHCS will maintain the final decision making over a breach determination.

D. ***Notification of Individuals***. When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County Department/Agency shall give the notice, subject to the following provisions:

1. If the cause of the breach is attributable to the County Department/Agency or its subcontractors, agents or vendors, the County Department/Agency shall pay any costs of such notifications, as well as any and all costs associated with the breach. If the cause of the breach is attributable to CDSS, CDSS shall pay any costs associated with such notifications, as well as any costs associated with the breach. If there is any question as to whether CDSS or the County Department/Agency is responsible for the breach, CDSS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs;

2. All notifications (regardless of breach status) regarding beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of 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 from discovery;

3. The CDSS Information Security and Privacy Bureau shall approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. If notifications are distributed without CDSS review and approval, secondary follow-up notifications may be required; and

4. CDSS may elect to assume responsibility for such notification from the County Department/Agency.

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/Agency or its agents, subcontractors or vendors, the County Department/Agency is responsible for all required reporting of the breach. If the cause of the breach is attributable to CDSS, CDSS is responsible for all required reporting of 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/Agency 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***. The County Department/Agency shall utilize the below contact information to direct all notifications of breach and security incidents to CDSS and DHCS. CDSS reserves the right to make changes to the contact information by giving written notice to the County Department/Agency. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

CDSS Information Security and Privacy Bureau	DHCS Breach and Security Incident Reporting
California Department of Social Services Information Security and Privacy Bureau 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558 *The preferred method of communication is email, when available. Do not include any PII unless requested by CDSS.*	Department of Health Care Services Office of HIPAA Compliance 1501 Capitol Avenue, MS 4721 P.O. Box 997413 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (866) 866-0602 *The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.*

XI.   <u>COMPLIANCE WITH SSA AGREEMENT</u>

The County Department/Agency agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS), in the Information Exchange Agreement (IEA) between SSA and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are hereby incorporated into this Agreement (Exhibit A) and available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, 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, CDSS will, as soon as reasonably possible after receipt, supply copies to the County Welfare Directors Association (CWDA) as well as the 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 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 County Department/Agency, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date, it shall submit a CAP to CDSS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential County Department/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County Department/Agency agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS, which is hereby incorporated into this Agreement (Exhibit B) and available upon request. 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/Agency, along with the compliance date expected by DHS-USCIS. If a County Department/Agency is not able to meet the DHS-USCIS compliance date, it shall 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/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XIII.   COUNTY DEPARTMENT/AGENCY AGENTS, SUBCONTRACTORS, AND VENDORS

The County Department/Agency agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to County Department/Agency PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the County Department/Agency with respect to PII upon such agents, subcontractors, and vendors. These shall include, at a minimum, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the County Department/Agency. If the agents, subcontractors, and vendors of County Department/Agency access data provided to DHCS and/or CDSS by SSA or DHS-USCIS, the County Department/Agency shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

County Department/Agency(s) who would like assistance or guidance with this requirement are encouraged to contact CDSS via email at cdsspsa@dss.ca.gov.

XIV.   ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the County Department/Agency agrees to assist CDSS or DHCS (on behalf of CDSS) in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the County Department/Agency, with reasonable notice from CDSS or DHCS. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The County Department/Agency agrees to promptly remedy all violations 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/Agency of the privacy or security of PII, or federal or state laws or agreements concerning privacy or security of PII, the County Department/Agency shall make all reasonable effort to make itself and County Workers 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/Agency at no cost to the County Department/Agency to testify as witnesses, in the event of litigation or administrative proceedings involving the County Department/Agency 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/Agency 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/Agency agrees to promptly enter into negotiations with CDSS concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. In addition to any other lawful remedy, CDSS may terminate this Agreement upon thirty (30) days written notice if the County Department/Agency does not promptly agree to 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 begin upon signature and approval of CDSS.

XVIII. TERMINATION

A. This Agreement shall terminate on **September 1, 2022**, 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 an executed written amendment. County Department/Agency requests for an extension shall be justified and approved by CDSS and limited to no more than a six (6) month extension.

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/Agency's possession shall continue in effect beyond the termination or expiration of this 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/Agency, CDSS may provide an opportunity for the County Department/Agency to cure the breach or end the violation and may terminate this Agreement if the County Department/Agency 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/Agency 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/Agency shall return or 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 returned or destroyed and CDSS receives a certificate of destruction.

XX. <u>SIGNATORIES</u>

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 **September 1, 2019**.

For the County of San Bernardino _____

Department/Agency of Human Services Group _____ ,

COUNTY OF SAN BERNARDINO	HUMAN SERVICES
	(Print or type name of corporation, company, contractor, etc.)

By ► _____

► _____
Curt Hagman, Chairman, Board of Supervisors

(Authorized signature - sign in blue ink)

Dated: _____

Name   CaSonya Thomas
(Print or type name of person signing contract)

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD
   Lynna Monell
   Clerk of the Board of Supervisors
   of the County of San Bernardino

Title   Assistant Executive Officer
_____
(Print or Type)

Dated: _____

By _____
      Deputy

Address   385 N. Arrowhead Ave., 5th Floor
    San Bernardino, CA 92415-0120

For the California Department of Social Services,

_____ _____

(Signature)   (Date)

_____ Chief, Contracts & Purchasing Bureau

(Name – Print or Type)   (Title – Print or Type)

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff from CDSS by emailing CDSS at cdsspsa@dss.ca.gov.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and CDSS (IEA-F and IEA-S)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff by emailing CDSS at cdsspsa@dss.ca.gov.

- 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)