PRIVACY AND SECURITY AGREEMENT
BETWEEN
the California Department of Social Services and the California Statewide Automated Welfare System Joint Powers Authority

PREAMBLE

The California Department of Social Services (CDSS) and the California Statewide Automated Welfare System Joint Powers Authority (CalSAWS Consortium) enter into this Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Social Security Administration (SSA) information, Medi-Cal Eligibility Data Systems (MEDS) information, Income and Eligibility Verification System (IEVS) and Personally Identifiable Information (PII). 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 CalSAWS Consortium is responsible for the maintenance and operation of the case management system used by County Departments/Agencies in their administration of the program. The case management system stores PII for the purpose of assisting the County Departments/Agencies with determining eligibility.

This Agreement covers the CalSAWS Consortium and its workers, who assist in the administration of; and access, use, or disclose PII.

The CalSAWS Consortium is accountable to County Departments/Agencies pursuant to law and/or one or more separate agreements, to which CDSS is not a party. County Departments/Agencies are accountable to CDSS for certain aspects of the administration of the program pursuant to law and separate agreements, to which the CalSAWS Consortium is not a party. This Agreement is not intended to diminish or supplant in any way the distinct relationships that the CalSAWS Consortium and CDSS each have with County Departments/Agencies but reflects the recognition of the parties

of the need for and desirability of a more direct relationship between them.

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, such as establishing eligibility, determining the amount of medical assistance, 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. **"Consortium Worker"** means those CalSAWS Consortium employees, contractors, subcontractors, vendors and agents performing any functions for the CalSAWS Consortium that require access to and/or use of PII and that are authorized by the CalSAWS Consortium to access and use PII. An agent is a person or organization authorized to act on behalf of the CalSAWS Consortium.

4. **" PII"** is information directly obtained in the course of performing an administrative function that can be used alone, or in conjunction with any other information, to identify a specific individual. Pll 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. Pll 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 CalSAWS Consortium, or a contractor, subcontractor or vendor of the CalSAWS Consortium.

6. **"Secure Areas"** means any area where:
    A. CalSAWS Consortium assist in the administration of;
    B. CalSAWS Consortium use or disclose Pll; 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).

AGREEMENTS

CDSS and CalSAWS Consortium mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. Consortium Workers may use or disclose PII only as permitted in this Agreement and only to assist in the administration of in accordance with Section 14100.2 of the Welfare and Institutions Code, Section 431.302 of Title 42 Code of Federal Regulations, as limited by this Agreement, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of a client, such as through an authorized release of information form, are allowable. Any other use or disclosure of PII requires the express approval in writing of CDSS. No Consortium Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

B. While CDSS is a covered entity under the federal Health Insurance Portability and Accountability Act, as amended from time to time (HIPAA), the CalSAWS Consortium is not required to be the business associate of CDSS, if the activities of the CalSAWS Consortium are limited to determining eligibility for, or enrollment in, (45 CFR 160.103). Nevertheless, it is the intention of the parties to protect the privacy and security of PII and the rights of applicants and beneficiaries in a manner that is consistent with HIPAA and other laws that are applicable. It is not the intention of the parties to voluntarily subject the CalSAWS Consortium to federal HIPAA jurisdiction where it would not otherwise apply, and CDSS does not assert any authority to do so.

1. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to PII covered under this Agreement beyond those provided through HIPAA, as applicable, CalSAWS Consortium shall:

    a. Comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals

whose information is concerned; and

b. Treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section VIII. of this Agreement. It is not the intention of the parties that this subsection I.B.(1)(b) expands the definitions of breach nor security incident set forth this Agreement unless the additional and/or more protective standard has a different definition for these terms, as applicable.

Examples of laws that provide additional and/or stricter privacy protections to certain types of PII include but are not limited to the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

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

D. Consortium 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 CalSAWS Consortium agrees to advise Consortium 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 CalSAWS Consortium shall implement the following personnel controls:

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

1. Provide initial privacy and security awareness training to each new Consortium Worker within 30 days of employment;

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

3. Maintain records indicating each Consortium 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 five years after completion of the training.

B. ***Employee Discipline***.

1. Provide documented sanction policies and procedures for Consortium 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 Consortium Workers sign a confidentiality statement. The statement shall be signed by Consortium Workers prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of five years.

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

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

D. ***Background Screening.***

1. Conduct a background screening of a Consortium 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 CalSAWS Consortium shall retain each Consortium Worker's background screening documentation for a period of three years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

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

A. Conduct periodic privacy and security review of work activity by Consortium 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.

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 the program and the use or disclosure of PII.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The CalSAWS Consortium 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 the CDSS with applicable contact information for these designated individuals using the County PSA inbox listed in Section IX of this Agreement. Any changes to this information should be reported to CDSS within ten days.

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

V. TECHNICAL SECURITY CONTROLS

The State of California Office of Information Security (OIS) and SSA have adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy controls for Information Systems and Organizations, and NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.

OIS and SSA require organizations to comply and maintain the minimum standards outlined in NIST SP 800-53 when working with PII and SSA data. CalSAWS Consortium shall, at a minimum, implement an information security program that effectively manages risk in accordance NIST SP 800-53, revision 5.

Guidance regarding implementation of NIST SP 800-53 is available in the Statewide Information Management Manual (SIMM), SIMM-5300-A, which is hereby incorporated into this Agreement (Exhibit C) and available upon request.

Minimum Cloud Security Requirements

CalSAWS Consortium and any agents, subcontractors, and vendors storing PII in a cloud service must comply with the Cloud Computing Policy, State Administration Manual (SAM) Sections 4983-4983.1, and employ the capabilities in the Cloud Security Standard, SIMM 5315-B to protect information and systems in cloud services as outlined below.

1. Identify and classify assets to focus and prioritize efforts in aligning business needs and risk management.
2. Each information asset for which the CalSAWS Consortium entity has ownership responsibility shall be inventoried and identified to include the following:
    a. Description and value of the information asset.

b. Owner of the information asset.
c. Custodians of the information asset.
d. Users of the information asset.
e. Classification of information.
f. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).
g. Importance of information assets to the execution of the Agency/state entity's mission and program function.
h. Potential consequences and impacts if confidentiality, integrity, and availability of the information asset were compromised.

3. Security of cloud services stems from managing authentication and fine-grained authorization. To safeguard cloud systems, CalSAWS Consortium shall establish processes and procedures to ensure:
    a. Maintenance of user identities, including both provisioning and de-provisioning;
    b. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
    c. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
    d. Separation of duties to avoid functional conflicts;
    e. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
    f. Use of privileged accounts that can bypass security are restricted and audited;
    g. Systems to administer access based on roles are defined and installed; and
    h. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

4. Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities. PaaS and SaaS resources may already have these controls implemented by the service provider. CalSAWS Consortium must configure information assets to provide only essential capabilities.
5. CalSAWS Consortium are entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed data storage services with native protection and backup features, but these features must be configured and managed appropriately.
6. Detective controls identify potential security threats or incidents, supporting timely investigation and response. CalSAWS Consortium must continuously identify and remediate vulnerabilities.
7. Response controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. Compliance with incident management requirements as outlined in VII. Notification and Investigation of Breaches and Security Incidents.
8. Recover controls facilitate long-term recovery activities following events or

incidents. With cloud services, primarily SaaS solutions, the services provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. CalSAWS Consortium must ensure agreements with cloud service providers include recover controls.

A. ***Minimum Necessary.*** Only the minimum necessary amount of PII required to perform required business functions applicable to the terms of this Agreement may be used, disclosed, copied, downloaded, or exported.

B. ***Transmission and Storage of PII.*** All persons that will be working with PII shall employ FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1 encryption of PII at rest and in motion unless CalSAWS Consortium determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, CalSAWS Consortium shall maintain, at a minimum, the most current industry standards for transmission and storage of CDSS data and other confidential information.

C. ***CDSS Remote Work Policy.*** CalSAWS Consortium, its Consortium Workers and any agents, subcontractors, and vendors accessing PII pursuant to this PSA when working remotely, shall follow reasonable policies and procedures that are equivalent to or better than the CDSS Remote Work Policy, as published in CDSS Telework Policy. Working remotely means working from a physical location not under the control of the person's employer.

If CDSS changes the terms of the CDSS Remote to Work Policy, CDSS will, as soon as reasonably possible, supply copies to CWDA and the CalSAWS Consortium or its designee as well as CDSS' proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CalSAWS Consortium or its designee on the proposed changes. If the CalSAWS Consortium is unable to comply with these standards, the CalSAWS Consortium will be asked to develop a Plan of Action and Milestones (POA&M) detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to CDSS for review and approval. Any CalSAWS Consortium who is under a POA&M will be required to provide quarterly updates to CDSS until fully compliant.

VI. AUDIT CONTROLS

A. ***Audit Control Mechanisms.*** The CalSAWS Consortium shall ensure audit control mechanisms are in place that are compliant with the Technical Security Controls within Section V of this Agreement.

B. ***Notification to CDSS in event CalSAWS Consortium is subject to other***

Audit. If CalSAWS Consortium is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of law related to the privacy and security of PII,the CalSAWS Consortium shall promptly notify CDSS unless it is legally prohibited from doing so.

VII. PAPER, RECORD, AND MEDIA CONTROLS

A. ***Supervision of Data.*** PII shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office at the individual's place of employment or at home when working remotely. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles.*** The CalSAWS Consortium shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Consortium Workers can transport PII, as well as the physical security requirements during transport. A CalSAWS Consortium that chooses to permit its Consortium Workers to leave records unattended in vehicles, 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.*** PII 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 crosscut shredding or pulverizing.

F. ***Removal of Data.*** PII shall not be removed from the premises of CalSAWS Consortium except for justifiable business purposes.

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 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.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the CalSAWS Consortium 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 The Department of Health Care Services:***
The Department of Health Care Services (DHCS) is acting on behalf of CDSS for purposes of processing reports of privacy and information security incidents and breaches. The CalSAWS Consortium shall notify DHCS using DHCS' online incident reporting portal of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII. When making notification, the following applies:

1. If a suspected security incident involves PII provided or verified by SSA, the CalSAWS Consortium 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 CalSAWS Consortium shall notify DHCS promptly and in no event later than one working day of discovery of:

    a. Unsecured PII if the PII is reasonably believed to have been accessed or acquired by an unauthorized person;
    b. Any suspected security incident which risks unauthorized access to PII and/or;
    c. Any intrusion or unauthorized access, use, or disclosure of PII in violation of this Agreement; or
    d. Potential loss of PII affecting this Agreement.

Notice to DHCS shall include all information known at the time the incident is reported. The CalSAWS Consortium can submit notice via the DHCS incident reporting portal which is available online at:
https://www.DHCS.ca.gov/formsandpubs/laws/priv/Pages/default.aspx

If DHCS' online incident reporting portal is unavailable, notice to DHCS can instead be made via email using the DHCS Privacy Incident Report (PIR) form. The email address to submit a PIR can be found on the PIR and in subsection H of this section. The CalSAWS Consortium shall use the most current version of the PIR, which is available online at: https://www.DHCS.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf.

If the CalSAWS Consortium is unable to notify DHCS the via the Incident Reporting Portal or email, notification can be made by telephone using the contact information listed in subsection H.

A breach shall be treated as discovered by the CalSAWS Consortium 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 CalSAWS Consortium.

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

1. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and

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

B. ***Investigation of Security Incident or Breach.*** The CalSAWS Consortium shall immediately investigate such a security incident, breach, or unauthorized use of PII.

C. ***Complete Report.*** Within ten (10) working days of the discovery the CalSAWS Consortium shall provide any additional information related to the incident requested by DHCS. The CalSAWS Consortium shall make reasonable efforts to provide DHCS with such information.

The complete report must include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable federal and state laws. The report shall include a full, detailed corrective action plan (CAP) including mitigating measures that were taken to halt and/or contain the improper use or disclosure.

If CDSS requests additional information related to the incident, the CalSAWS Consortium shall make reasonable efforts to provide DHCS with such information. If necessary, the CalSAWS Consortium shall submit an updated report 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. CDSS will maintain the final decision making over a breach determination.

D. ***Notification of Individuals.*** If the cause of a breach is solely attributable to CalSAWS Consortium or its agents, CalSAWS Consortium shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made. DHCS and the CalSAWS Consortium shall work together to ensure that notification of individuals is done in compliance with statutory deadlines within applicable federal and state law.

If the cause of a breach is solely attributable to DHCS or CDSS, DHCS or CDSS shall pay all costs of such notifications as well as any costs associated with the breach.
If there is any question as to whether DHCS, CDSS or the CalSAWS Consortium is responsible for the breach or DHCS, CDSS and the CalSAWS Consortium acknowledge that both are responsible for the breach, DHCS, CDSS and the CalSAWS Consortium shall jointly determine responsibility for purposes of allocating the costs.

1. 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.

E. ***Responsibility for Reporting of Breaches***

1. ***Breach Attributable to CalSAWS Consortium.*** If the cause of a breach of PII is attributable to the CalSAWS Consortium or its agents, subcontractors, or vendors, the CalSAWS Consortium shall be responsible for all required reporting of the breach.

2. ***Breach Attributable to DHCS or CDSS.*** If the cause of the breach is attributable to DHCS or CDSS, DHCS or CDSS shall be responsible for all required reporting of the breach.

F. ***Coordination of Reporting.*** When applicable law requires the breach be reported to a federal or state agency, or that notice be given to media outlets, CDSS and the CalSAWS Consortium shall coordinate to ensure such reporting is compliant with applicable law and prevent duplicate reporting and to jointly determine responsibility for purposes of allocating

the costs of such reports, if any.

G. ***Submission of Sample Notification to Attorney General:*** If the cause of the breach is attributable to the CalSAWS Consortium or an agent, subcontractor, or vendor of the CalSAWS Consortium and if notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, regardless of whether CalSAWS Consortium is considered only a custodian and/or non-owner of the PII, CalSAWS Consortium shall, at its sole expense and at the sole election of CDSS, either:

1. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). CalSAWS Consortium shall inform the CDSS Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or

2. Cooperate with and assist CDSS in its submission of a sample copy of the notification to the Attorney General.

H. ***DHCS Contact Information.*** The CalSAWS Consortium shall utilize the below contact information to direct all communication/notifications of breach and security incidents to CDSS. CDSS reserves the right to make changes to the contact information by giving written notice to the CalSAWS Consortium. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

DHCS Breach and Security Incident Reporting
Department of Health Care Services Privacy Officer c/o Data Privacy Unit P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (916) 445-4646 *The preferred method of communication is email, when available. Do not include any PII unless requested by DHCS.*

Copy CDSS at:

CDSS Breach and Security Incident Reporting
California Department of Social Services Information Security and Privacy Bureau – CalSAWS PSA 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558

IX. CDSS PSA CONTACTS

The CalSAWS Consortium shall utilize the below contact information for any PSA-related inquiries or questions. CDSS reserves the right to make changes to the contact information by giving written notice to the CalSAWS Consortium. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated. *Please use the contact information listed in Section X of this Agreement for any PII incident or breach reporting.*

PSA Inquires and Questions
California Department of Social Services Information Security and Privacy Bureau – CalSAWS PSA 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413 Email: iso@dss.ca.gov Telephone: (916) 651-5558

X. COMPLIANCE WITH SSA AGREEMENT

The CalSAWS Consortium agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CalHHS), 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 incorporated into this Agreement within section V. Technical Security Controls and Exhibit A (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 CalSAWS Consortium as well as CDSS' proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CalSAWS Consortium 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 CalSAWS Consortium, along with the compliance date expected by SSA. If the CalSAWS Consortium is not able to meet the SSA compliance date, the CalSAWS Consortium will be asked to develop a POA&M detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to CDSS for review and approval. Any CalSAWS Consortium who is under a POA&M will be required to provide quarterly updates to CDSS until the fully compliant.

A copy of Exhibit A can be requested by authorized CalSAWS Consortium individuals from CDSS using the contact information listed in Section XI of this Agreement.

XI. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The CalSAWS Consortium 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 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 the CalSAWS Consortium as well as CDSS' proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CalSAWS Consortium on the proposed target date and make adjustments, if appropriate. After the 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 CalSAWS Consortium, along with the compliance date expected by DHS-USCIS. If the CalSAWS Consortium is not able to meet the DHS-USCIS compliance date, the POA&M must be provided to CDSS for review and approval. Any CalSAWS Consortium who is under a POA&M will be required to provide quarterly updates to CDSS until the fully compliant.

A copy of Exhibit B can be requested by authorized CalSAWS Consortium individuals from CDSS using the contact information listed in Section IX of this Agreement.

XII. CALSAWS CONSORTIUM'S AGENTS, SUBCONTRACTORS, AND VENDORS

The CalSAWS Consortium agrees to enter into written agreements with all agents, subcontractors and vendors that have access to CalSAWS Consortium PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the CalSAWS Consortium with respect to PII upon such agents, subcontractors, and vendors. These shall include, (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 CalSAWS Consortium. If the agents, subcontractors, and vendors of CalSAWS Consortium access data provided to CDSS and/or CDSS by SSA or DHS-USCIS, the CalSAWS Consortium shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

CalSAWS Consortium who would like assistance or guidance with this requirement are encouraged to contact CDSS via the PSA inbox at CountyPSA@CDSS.ca.gov.

XIII. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the CalSAWS Consortium agrees to assist CDSS in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the CalSAWS Consortium, with reasonable notice from CDSS. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The CalSAWS Consortium agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the CDSS Privacy Office and CDSS Information Security Office in writing, or to enter into a POA&M with CDSS containing deadlines for achieving compliance with specific provisions of this Agreement.

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XV. AMENDMENT OF AGREEMENT

CDSS and the CalSAWS Consortium acknowledge that federal and state laws relating

to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such changes. Upon request by CDSS, the CalSAWS Consortium agrees to promptly enter into negotiations with CDSS concerning an amendment to this Agreement as may be needed by changes in federal and state laws and regulations or NIST 800-53. In addition to any other lawful remedy, CDSS may terminate this Agreement upon 30 days written notice if the CalSAWS Consortium 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.

XVI. TERMINATION

This Agreement shall terminate on September 1, 2028, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement. CalSAWS Consortium's requests for an extension shall be approved by CDSS and limited to no more than a six (6) month extension.

A. ***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 CalSAWS Consortium'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.

XVII. TERMINATION FOR CAUSE

Upon CDSS' knowledge of a material breach or violation of this Agreement by the CalSAWS Consortium, CDSS may provide an opportunity for the CalSAWS Consortium to cure the breach or end the violation and may terminate this Agreement if the CalSAWS Consortium 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 CalSAWS Consortium 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 CalSAWS Consortium shall return or destroy all PII in accordance with Section VII, 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.

XVIII. 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 September 1, 2024.

For the California Statewide Automated Welfare System Joint Powers Authority,

(Signature)	(Date)
(Name)	(Title)

For the Department of Social Services,

(Signature)	(Date)
Jennifer Troia	Director
(Name)	(Title)

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the CalSAWS Consortium information security and privacy staff, or other authorized county official from CDSS by using the contact information listed in Section IX of this Agreement.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and CDSS
- 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 CalSAWS Consortium information security and privacy staff, or other authorized county official from CDSS by using the contact information listed in Section IX of this Agreement.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and California Department of Social Services (CDSS)

EXHIBIT C

Exhibit C consists of the current version of the SIMM-5300-A, a copy of which can be requested by the CalSAWS Consortium information security and privacy staff, or other authorized county official from CDSS by using the contact information listed in Section IX of this Agreement. The SIMM-5300-A can be used as guidance for implementing security controls found in NIST SP 800-53.