

**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 (PSA) in order to ensure the privacy and security of Social Security Administration (SSA) information, Medi-Cal Eligibility Data Systems information, Income and Eligibility Verification System and Personally Identifiable Information (PII). This PSA covers the following programs:

- CalFresh;
- California Food Assistance Program;
- California Work Opportunity and Responsibility to Kids Program;
- Cash Assistance Program for Immigrants;
- Entrant Cash Assistance/Refugee Cash Assistance;
- Foster Care (eligibility);
- Kinship Guardianship Assistance Program (eligibility);
- Federal Guardianship Assistance Program (eligibility);
- General Assistance/General Relief; and
- Trafficking and Crime Victims Assistance Program.

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 PSA 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.

The PSA 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 PSA, the following terms mean:

1. Assist in the administration of the program

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

The 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

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

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. 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

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

Any area where:

- a. CalSAWS Consortium assist in the administration of;
- b. CalSAWS Consortium use or disclose PII; or
- c. PII is stored in paper or electronic format.

7. SSA-provided or verified data (SSA data)

SSA Data means:

- a. Any information under the control of the 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:

PRIVACY AND CONFIDENTIALITY

1. Consortium Workers may use or disclose PII only as permitted in this PSA 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 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 PSA.
2. Access to PII shall be restricted to Consortium Workers who need to perform their official duties to assist in the administration of the programs.
3. Consortium Workers who access, disclose or use PII in a manner or for a purpose not authorized by this PSA may be subject to civil and criminal sanctions contained in applicable federal and State statutes.

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:

1. Employee Training

Train and use reasonable measures to ensure compliance with the requirements of this PSA by Consortium Workers, including, but not limited to:

- a. Provide initial privacy and security awareness training to each new Consortium Worker within 30 days of employment;
- b. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this PSA to all Consortium Workers. Three or more security reminders per year are recommended;
- c. Maintain records indicating each Consortium Worker's name and the date on which the privacy and security awareness training was completed and;
- d. Retain training records for a period of five years after completion of the training.

2. Employee Discipline

- a. Provide documented sanction policies and procedures for Consortium Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.
- b. Sanction policies and procedures shall include termination of employment when appropriate.

3. 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.

- a. The statement shall include, at a minimum, a description of the following:
 - i. General Use of PII;
 - ii. Security and Privacy Safeguards for PII;
 - iii. Unacceptable Use of PII; and
 - iv. Enforcement Policies.

4. Background Screening

- a. Conduct a background screening of a Consortium Worker before they may access PII.
- b. 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.

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

I. MANAGEMENT OVERSIGHT AND MONITORING

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

1. 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.
2. 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:

1. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this PSA.
2. Provide the CDSS with applicable contact information for these designated individuals using the County PSA inbox listed in Section IX of this PSA. Any changes to this information should be reported to CDSS within ten days.
3. Assign Consortium Workers to be responsible for administration and monitoring of all security-related controls stated in this PSA.

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 PSA (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. The CalSAWS Consortium must configure information assets to provide only essential capabilities.

5. The CalSAWS Consortium is 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. The 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. The CalSAWS Consortium must ensure agreements with cloud service providers include recover controls.

Minimum Necessary

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

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.

The 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 (POAM) detailing a concrete roadmap to becoming fully compliant with the policy's standard.

The POAM must be provided to CDSS for review and approval. If CalSAWS Consortium is under a POAM, they will be required to provide quarterly updates to CDSS until fully compliant.

VI. AUDIT CONTROLS

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 PSA.

Notification to CDSS in event CalSAWS Consortium is subject to other Audits

If the 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 PSA 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

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.

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. If CalSAWS Consortium 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.

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.

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.

Confidential Destruction

PII shall be disposed of through confidential means, such as crosscut shredding or pulverizing.

Removal of Data

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

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.

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 PSA, 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:

1. **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.
2. 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:
 - a. 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 PSA.

- b. 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:
 - i. Unsecured PII if the PII is reasonably believed to have been accessed or acquired by an unauthorized person;
 - ii. Any suspected security incident which risks unauthorized access to PII and/or;
 - iii. Any intrusion or unauthorized access, use, or disclosure of PII in violation of this PSA; or
 - iv. Potential loss of PII affecting this PSA.
- c. 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](#).
- d. 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](#).
- e. 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.
- f. 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.
- g. Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the CalSAWS Consortium shall take:
- h. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and
- i. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

3. Investigation of Security Incident or Breach

The CalSAWS Consortium shall immediately investigate such a security incident, breach, or unauthorized use of PII.

4. Complete Report

Within ten (10) working days of the discovery of a security incident, breach, or unauthorized use of PII, 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.

- a. 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 including mitigating measures that were taken to halt and/or contain the improper use or disclosure.

- b. 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.

5. Notification of Individuals

If the cause of a breach is solely attributable to the CalSAWS Consortium or its agents, the 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.

- a. 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.
- b. 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.
- c. 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.

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.

3. 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.

4. 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:

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

5. 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 PSA 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 9-10-59
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 PSA or any other agreement into which it is incorporated. Please use the contact information listed in Section X of this PSA 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 9-10-59
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, 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 PSA 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 PSA, 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 adjust, 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 POAM detailing a concrete roadmap to becoming fully compliant with the policy's standard.

The POAM must be provided to CDSS for review and approval. If CalSAWS Consortium is under a POAM, they 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 PSA.

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 PSA (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 PSA, 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 adjust, 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 POAM must be provided to CDSS for review and approval. If the CalSAWS Consortium is under a POAM, they will be required to provide quarterly updates to CDSS until 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 PSA.

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 PSA's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

If CalSAWS Consortium 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 PSA 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 consider the operational and staffing demands. The CalSAWS Consortium agrees to promptly remedy all violations of any provision of this PSA and certify the same to the CDSS Privacy Office and CDSS Information Security Office in writing, or to enter into a POAM with CDSS containing deadlines for achieving compliance with specific provisions of this PSA.

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 PSA 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 PSA 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 PSA upon 30 days written notice if the CalSAWS Consortium does not promptly agree to enter into negotiations to amend this PSA when requested to do so or does not enter into an amendment that CDSS deems necessary.

XVI. TERMINATION

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

- **Survival:** All provisions of this PSA 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 PSA 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 PSA 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 PSA if the CalSAWS Consortium does not cure the breach or end the violation within the time specified by CDSS. This PSA 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 PSA, the CalSAWS Consortium shall return or destroy all PII in accordance with Section VII, above.

The provisions of this PSA 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.

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 PSA.

- 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

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 PSA.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services and California Department of Social Services

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 PSA. The SIMM-5300-A can be used as guidance for implementing security controls found in NIST SP 800-53.

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 PSA.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this PSA. 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)	10/8/2025 _____ (Date)
---	------------------------------

Jennifer Troia _____ (Name)	Director _____ (Title)
-----------------------------------	------------------------------