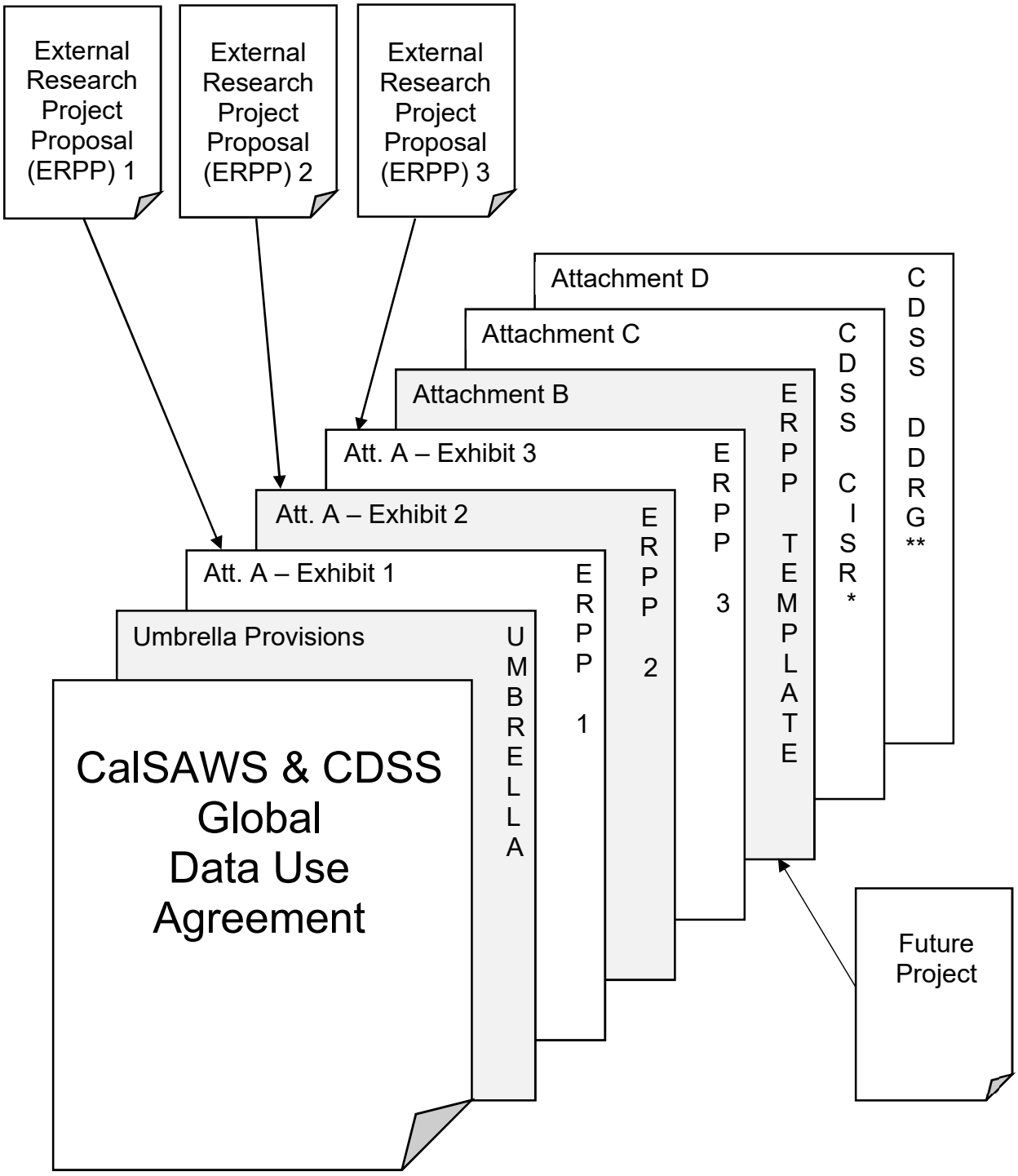
Global Data Use Agreement between
California Statewide Automated Welfare System Consortium (CalSAWS)
and California Department of Social Services (CDSS)



* CDSS Confidentiality and Information Security Requirements
** CDSS Data De-Identification Reference Guide

GLOBAL DATA USE AGREEMENT
BETWEEN
CALIFORNIA STATEWIDE AUTOMATED WELFARE SYSTEM CONSORTIUM
AND
CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

This Global Data Use Agreement (DUA) is entered into by and between the California Department of Social Services (CDSS) and the California Statewide Automated Welfare System (CalSAWS) Consortium as of [Enter Date]. CDSS and the CalSAWS Consortium may be referred to herein as "Party" and collectively as "Parties".

I. PURPOSE

This DUA is intended to be the sole agreement by which the CDSS obtains county data ("SAWS data") from the CalSAWS Consortium to provide to approved External Researchers for approved purposes ("External Research Project"). The process provided for in this DUA is intended to align with the current review and approval process for SAWS data sharing and the current process for the CalSAWS Joint Powers Authority (JPA) consent. The goal of this DUA is to streamline the process for SAWS data sharing without the need to enter into separate agreements for each External Research Project, except where a different agreement is required by federal or state law.

This DUA consists of the terms and conditions set forth in Sections I through IX herein, Attachment A, Approved External Research Project Proposal (ERPP), Attachment B, ERPP Template, Attachment C, CDSS Confidentiality and Information Security Requirements (CISR), Attachment D, CDSS Data De-Identification Reference Guide (DDRG).

II. BACKGROUND AND AUTHORITY

A. This DUA 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); and
- Trafficking and Crime Victims Assistance Program (TCVAP).

B. CDSS is the state agency responsible for the administration of social services programs in California.

C. The CalSAWS Consortium established itself as a Joint Powers Authority (JPA) by agreement with the 58 California Counties to provide a single

legal entity for purposes of managing the C-IV, CalWIN, and LRS Systems that maintain the client data of each County. The client data may include data from the CDSS Programs listed in Section II., Paragraph A above. The client data is confidential data as specified in Welfare and Institutions Code (WIC) section 10850 and is required to be protected from unauthorized access in accordance with state and federal laws.

D. WIC section 10850 specifically authorizes any County Welfare Department (CWD) in the state to provide "… lists of applicants for, or recipients of, public social services, to any other county welfare department or the State Department of Social Services, and these lists or any other records shall be released when requested by the State Department of Social Services. These records shall only be used for purposes directly connected with the administration of public social services".

WIC section 10850, subdivision (g) authorizes the CDSS to make case records available for research purposes if the requestor has complied with subdivision (t)(1) of Section 1798.24 of the Civil Code. This subdivision allows for the provision of confidential information to the University of California, a non-profit educational institution, an established non-profit research institution performing health or social services research, the Cradle-to-Career Data System, for purposes consistent with the creation and execution of the Cradle-to-Career Data System Act pursuant to Article 2 (commencing with Section 10860) of Chapter 8.5 of Part 7 of Division 1 of Title 1 of the Education Code, or, in the case of education-related data, another nonprofit entity, conducting scientific research, provided the request for information is approved by the Committee for the Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CalHHS).

E. No part of this agreement should be construed to limit the CDSS' existing statutory authority through WIC 10850 to access and make case records available for research purposes.

III. SCOPE OF WORK

A. Under this DUA, the CDSS and the CalSAWS Consortium agree to work together, in collaboration with the requesting External Researchers, to create ERPPs to facilitate the exchange of the SAWS data from the CalSAWS Consortium to the CDSS so it can be shared with External Researchers for the specific purpose of research.

B. All ERPPs subject to this DUA will be contained in project-specific exhibits in Attachment A, which is attached hereto and by this reference incorporated herein. The ERPPs may be added to and included in Attachment A pursuant to Paragraph C, without amending this DUA.

C. In order to add a new ERPP to this DUA, the CDSS will use the ERPP Template in Attachment B, which is attached hereto and by this reference incorporated herein, to create a project-specific exhibit. If mutually agreed upon by the CalSAWS Consortium and the CDSS or their respective designees, as evidenced by their signatures on the applicable ERPP, the new ERPP will be incorporated into this DUA as the next-in-sequence numbered exhibit to Attachment A (e.g., "ERPP 5" will be added as Attachment A, Exhibit 5).

D. The ERPP Template contains sections specifically included to allow for the addition of project-specific information that is not otherwise captured in one of the other sections of the Template.

E. The ERPP will include any additional exhibits that accompany the ERPP, such as the Committee for the Protection of Human Subjects (CPHS) Institutional Review Board (IRB) approval.

F. The ERPP included as an exhibit in Attachment A may be modified at any time by agreement of the Parties as evidenced by the signatures of authorized representatives of the CalSAWS Consortium and the CDSS, on the modified ERPP. The modified ERPP will replace the current ERPP being modified. An ERPP may be terminated pursuant to the terms set forth in the applicable ERPP. When an ERPP has been terminated, it shall be removed from this DUA.

IV. CDSS RESPONSIBILITIES

A. CDSS will receive a SAWS data request from an External Researcher and instruct them to draft the ERPP. As part of the draft ERPP, the External Researcher will confirm what level of reporting the project requires: state level, consortium level, and/or county level.

B. CDSS will assess the draft ERPP to ensure the proposed research meets the requirements of Section 1798.24 of the Civil Code, which include, but are not limited to, (1) the research is approved by the Committee for the Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CHHSA) or an institutional review board, (2) the requested data is limited to that necessary for the purpose of the research, and (3) sufficient administrative, physical, and technical safeguards are required to prevent the unauthorized disclosure of the data.

C. Once the CDSS has completed its review in B, the CDSS will provide the CalSAWS Consortium with the draft ERPP to review and verify the CalSAWS Consortium's ability to provide the requested SAWS data.

D. CDSS will coordinate any meetings with the External Researcher and the CalSAWS Consortium to discuss the ERPP prior to execution or as requested by the CalSAWS Consortium.

E. Upon agreement of final ERPP language, the CDSS will provide a final copy of the ERPP to the CalSAWS Consortium and the External Researcher for review and signature.

F. CDSS will provide the requested SAWS data to the External Researcher as specified in the executed ERPP.

G. CDSS will enter into a separate agreement with the External Researcher that ensures the External Researcher will follow the terms established in this DUA and its Attachments. This separate agreement will require the External Researcher to defend, indemnify, and hold harmless both the CalSAWS Consortium and any County(ies) whose data is released to the External Researcher from any claims or liabilities arising from unauthorized use or disclosure of SAWS data released to the External Researcher.

H. CDSS will require the External Researcher to certify that it complies with all data security and privacy requirements for the SAWS data.

I. CDSS will require the External Researcher to include on all publications a disclaimer that states, but is not limited to:

> "The findings reported herein were performed with the permission of the CDSS. The opinions and conclusions expressed herein are solely those of the authors and should not be considered as representing the views, policy or opinion of the CDSS, the California Health and Human Services Agency, any department or agency of the California government, or the CalSAWs Consortium. Additional information may be found at www.[insert URL].ca.gov."

The specific URL will be provided for the researcher prior to the date the publication will be issued, posted, presented, or the like.

J. CDSS will require the External Researcher to submit draft publications to the CDSS and the CalSAWS Consortium at least thirty (30) calendar days prior to the date the publication is scheduled to be issued, posted, presented, or the like. CDSS and the CalSAWS Consortium will have ten (10) business days from receipt to provide feedback. If the CDSS and/or the CalSAWS Consortium note the draft contains factual errors, such as misinterpretation or misunderstanding of what a data field represents, the parties must work with the External Researcher to correct the errors. Any disagreement between the External Researcher, on the one hand, and the

CalSAWS Consortium and/or County(ies), on the other hand, regarding the factual nature of the report must be resolved to the parties' mutual satisfaction before the report can be published. If the disagreement is not resolved, the ERPP must be terminated, all data must be returned, and the draft report must not be published. For all other disputes, the External Researcher is required to include a disclaimer in the final published report in accordance with scholarly standards.

V. CALSAWS CONSORTIUM RESPONSIBILITIES

A. The CalSAWS Consortium will review the draft ERPP for completeness, alignment with the terms of the Global DUA, and verify the requested SAWS data is available.

B. The CalSAWS Consortium shall have the right to reject an ERPP based on its determination that the ERPP does not meet the requirements of Section IV(B) or is otherwise statutorily impermissible, creates too great a risk of unauthorized disclosure of Confidential Data, or for other reasonable grounds as articulated by the CalSAWS Consortium. No SAWS data shall be available to an External Researcher prior to, or absent, the express approval of an ERPP by the CalSAWS Consortium. The CalSAWS Consortium will not unreasonably withhold its approval of an ERPP and, in the case that the CalSAWS Consortium rejects an ERPP, the CalSAWS Consortium will provide both the CDSS and the External Researcher with a written statement of its reasons for rejecting the ERPP. The CalSAWS Consortium will not unreasonably reject or withhold its approval of an ERPP.

C. If the CalSAWS Consortium disagrees with the CDSS that the draft ERPP meets the requirements of Section IV(B), the CalSAWS Consortium will notify the CDSS of this disagreement within five (5) business days of receipt of the draft ERPP. The CalSAWS Consortium and the CDSS Research, Automation, and Data Division's (RADD) Deputy Director will first attempt to resolve the issue informally. If an agreement is not reached through the informal discussion, the CalSAWS Consortium may request a formal written decision from the CDSS Executive Office within twenty (20) business days of receipt of the draft ERPP.

The CalSAWS Consortium will sign the ERPP within ten (10) business days of receipt of the draft ERPP or within five (5) business days after any disagreement is reconciled, whichever is later.

D. Upon the execution of each ERPP, the CalSAWS Consortium agrees to provide to the CDSS the SAWS data identified in the specific ERPP within the timeframes specified in the Critical Dates Section of the ERPP. If the CDSS is pulling the data directly, the CalSAWS Consortium agrees to provide and/or validate the required query needed to do so. CDSS shall

only use the provided files from the CalSAWS Consortium or data pulled via validated queries to transmit to the designated External Researcher for the purposes of fulfilling the requirements specified under the relevant ERPP.

E. The CalSAWS Consortium agrees to use secure file transfer protocols and encryption that meet or exceed the standards described in Attachment C, CDSS Confidentiality and Information Security Requirements.

VI. CONTACTS

A. The following CDSS representative is authorized to implement the terms and conditions of the DUA and will be responsible for the oversight and supervision of the security and confidentiality of the SAWS data sent to the CDSS by the CalSAWS Consortium:

Julianna Vignalats, Assistant Deputy Director
Chief Agency and State Data Liaison
Research, Automation, and Data Division
California Department of Social Services
744 P St. MS 8-5-41
Sacramento, CA 95814
Julianna.Vignalats@dss.ca.gov

B. The following CDSS representative will serve as the point of contact for communication between the CDSS and the CalSAWS Consortium:

Stace McClaflin, SSMI, Specialist
Data Stewardship Section
Research, Automation, and Data Division
California Department of Social Services
744 P St. MS 8-5-26
Sacramento, CA 95814
Stace.Mcclaflin@dss.ca.gov

C. The following CDSS representative will serve as the technical point of contact for this DUA:

Aparna Ramesh, Acting Data Coordinator
Chief, Research and Data Insights Branch
Research, Automation, and Data Division
California Department of Social Services
744 P St. MS 8-5-41
Sacramento, CA 95814
Aparna.Ramesh@dss.ca.gov

D. The following representative of the CalSAWS Consortium is authorized to implement the terms and conditions of the DUA and will be responsible for the oversight and supervision of the security and confidentiality of the transmission of SAWS data sent by the CalSAWS Consortium to the CDSS:

Laura Chavez
CalSAWS, Technical & Operations Director
12440 Imperial Hwy, 3rd Floor
Norwalk, CA 90650
(562) 484-7812
ChavezL@CalSAWS.org

E. Either Party may make changes to the contacts for this DUA within five (5) days advance written notice to the other. Said changes shall not require an amendment to this DUA.

VII. TERM

This DUA shall be effective on [Enter Date] or upon execution by the last to sign of the authorized representatives of the CDSS and the CalSAWS Consortium, whichever is later. The DUA shall extend indefinitely, unless terminated pursuant to Section VIII, paragraph B below.

VIII. GENERAL PROVISIONS

A. AMENDMENTS. This DUA may be amended in writing at any time by written mutual consent of the Parties.

B. TERMINATION.

1. Termination without cause: This DUA and all its attachments, including active ERPPs may be terminated by either Party without cause upon thirty (30) days' written notice. In the event this DUA is terminated prior to the execution of any ERPP, the termination will automatically act as a rejection of the unexecuted ERPP.

2. Termination with cause: This DUA may be terminated immediately by either Party if the terms of this DUA are violated by the other Party in any manner.

3. Other grounds for termination: In the event that any other contract, agreement or DUA which is identified in Section II. Background and Authority above, as being related to or necessary for the performance of this DUA, terminates or expires, this DUA may be terminated upon the effective date of the termination of that contract, agreement, or DUA, even if such termination will occur with less than thirty (30) days' written notice.

In the event this DUA is terminated pursuant to any of the Subparagraphs 1 through 3 above, all unused SAWS data in the possession of an External Researcher must be returned or destroyed in accordance with the Confidentiality and Information Security Requirements (Attachment C). CDSS will notify the CalSAWS Consortium that all SAWS data provided to an External Researcher under this DUA has either been returned or destroyed upon the termination in accordance with the Confidentiality and Information Security Requirements (Attachment C).

C. CONFIDENTIALITY AND INFORMATION SECURITY. CDSS will require External Researchers to comply with the CDSS Confidentiality and Information Security Requirements Exhibit, which is attached hereto as Attachment C. CDSS will require External Researchers to de-identify any summary data to be included in publications in accordance with the CDSS Data De-Identification Reference Guide, which is attached hereto as Attachment D.

CDSS will require the External Researcher 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 Agreements (IEA) between SSA and the CDSS, and in the most current Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are hereby incorporated into this DUA and available upon request. If there is any conflict between a privacy and security standard in the CMPPA, IEAs, or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard that provides the greatest protection to PII.

IX. REPRESENTATIVES

By signing below, the individual certifies that it is acting as the representative of the Party named below and possesses the authority to enter into this DUA on behalf of that Party and that the Party possesses the legal authority to enter into this DUA.

For CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

Ryan Gillette
Deputy Director, Chief Data Officer
Research, Automation, and Data Division
California Department of Social Services
744 P St.
Sacramento, CA 95814
Ryan.Gillette@dss.ca.gov

Signature: _____ **Date:** _____
Ryan Gillette, Deputy Director

For the CalSAWS CONSORTIUM

Michael J. Sylvester II, Assistant Director, Bureau of Special Operations
County of Los Angeles, Department of Public Social Services
12860 Crossroads Parkway South Floor: Main Office/Room: M-258
City of Industry, CA 91746
(562) 908-8644 - Office, (562) 207-8753 - Mobile
MichaelSylvester@dpss.lacounty.gov

John Boule, Executive Director
11290 Pyrites Way, Suite 150
Rancho Cordova, CA 95670
(916) 851-3201
BouleJ@calsaws.org

Signature: _____ **Date:** _____
Michael J. Sylvester II, Assistant Director

Signature: _____ **Date:** _____
John Boule, Executive Director

Approved as to legal form:

Signature: _____ **Date:** _____
Jeffrey Mitchell, CalSAWS Legal Counsel

CalSAWS External Research Project Proposal (ERPP) Template

CalSAWS External Research Project Proposal (ERPP) No. Enter next-in-sequence number
See Appendix A for definitions.

ERPP Form Fields	Field Description
External Research Project Name	Title for the External Research Project
Contact Information	California Department of Social Services (CDSS) Name, Division/Branch/Section, Email, Phone of person submitting proposal Name, Email, Phone of manager External Researcher (Data Recipient): Name, Organization, Email, Phone of person submitting proposal Name, Email, Phone of manager California Statewide Automated Welfare System (CalSAWS) Consortium Data Provider: Name, Division/Branch/Section, Email, Phone of person receiving proposal Name, Email, Phone of manager
External Research Project Description/Purpose	A general description of: • The scope for this External Research Project • The reason for this External Research Project request • Explanation as to why the External Researcher needs the SAWS data • The External Research Project benefits to CDSS, and the External Researcher, and SAWS data subjects (clients/customers)
Data Types/Categories	A high-level description of the types of SAWS data requested
Output/Use	A description of how the SAWS data will be used and resulting outputs: • What are the anticipated intermediate and final work products? Will those work products be public or non-public? • What analysis or decision-support will be produced? • What level will the findings be reported: statewide, consortium, county, and/or zip code level?

CalSAWS External Research Project Proposal (ERPP) Template

Data Elements	A detailed list of the SAWS data elements being requested
External Researchers	A description of: • Who will have access to the SAWS data, including confidential data? • Roles & Responsibilities of the External Researchers involved with the project • Whether contractors and/or subcontractors will have access to and use of the SAWS data
Data Transfer/Management	A description of how the SAWS data will be transferred, stored, and managed **Note:** Social Security Administration (SSA) provided data cannot be stored in a cloud hosted environment without review and approval from SSA.
Destruction and/or Return	A description of: • How the SAWS data will be destroyed or returned at the termination of the ERPP • Whether work products created with the SAWS data will be destroyed or returned • Any limitations on the use of the work products at the termination of the ERPP
Legal Authority	A description, if any, of additional legal authority that may apply due to: • CDSS' authority to provide the SAWS data to External Researchers for access and use • CalSAWS Consortium's authority to disclose/share **Note:** This should be filled out to the extent there is additional legal authority for this particular ERPP that is not covered by the authority in the umbrella document. Otherwise, N/A.
Critical Dates	A description of: • Deadlines (including start date and end date of the SAWS data request and timeframe that the requested SAWS data needs to be provided) • Timeframe for the use of the SAWS data for the External Research Project • Establish whether this is on-going or one-time SAWS data request; for on-going, indicate the frequency of the SAWS data request
CPHS IRB Approval for Research	• Committee for the Protection of Human Subjects (CPHS) Institutional Review Board (IRB) approval letter is attached in Appendix X
Specialized Privacy	A description, if any, of any specialized or additional privacy requirements that may apply due to: • Federal government, law, or policy

CalSAWS External Research Project Proposal (ERPP) Template

	• Contractual obligation • State government, law, or policy
Specialized Security	A description, if any, of any specialized or additional security requirements that may apply due to: • Federal government, law, or policy • Contractual obligation • State government, law, or policy
Approvals	Acknowledgement that the External Research Project is approved. • Name, title, email, phone number of approvers from CDSS, CalSAWS Consortium Data Management Board (CalSAWS DMB), and External Research Organization • Approver should be Chief Deputy Director or Program Deputy Director level or someone who has authority to sign agreements • Include Date Signed for all signatories **CDSS Approver:** Julianna Vignalats, Assistant Deputy Director Chief Agency and State Data Liaison Research, Automation, and Data Division 916-838-7017 Julianna.Vignalats@dss.ca.gov Signature: _____ Date signed: _____ **CalSAWS Consortium DMB Approver:** XXXXX, Title XXXXXX Division California Statewide Automated Welfare System Consortium Phone: Email:

CalSAWS External Research Project Proposal (ERPP) Template

	Signature: _____ Date signed: _____ **External Research Organization Approver:** XXXXX, Title Organization Name Phone: Email: Signature: _____ Date signed: _____

This External Research Project Proposal does not modify or alter any terms and conditions in the CalSAWS Consortium Global Data Use Agreement.

CalSAWS External Research Project Proposal (ERPP) Template

Appendix A: Additional Terms for Clarity

External Researcher (Data Recipient): External Research Organization that has been approved to access or receive SAWS data via CDSS.

Data Provider: CalSAWS Consortium Sponsor that provides access to the SAWS data to CDSS for the ERPP.

Research: a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to the generalizable knowledge.[1] For purposes of ERPPs, research does NOT include:

(i) Quality improvement or assurance activities
(ii) Public health or health services activities designed to protect the public's health or for normal program functions
(iii) Any study or activity specific to or for a program's normal operations
(iv) Health care operations activities, such as activities for case management and care coordination, business planning and development, management and administration, or program evaluation or assessment
(v) Health oversight activities, including Federal program or grant oversight, audits, or investigations related to law enforcement, fraud and abuse, licensing and professional discipline

An activity may fall both in and out of the research definition depending on purpose, who conducts it, funding, and whether the activity is required by law.[2]

[1] *See* 45 C.F.R. § 46.102(l).
[2] Public Health Data Standards Consortium. "PRISM, A Privacy Toolkit for Public Health Professionals." 2007.

The California Department of Social Services
Confidentiality and Information Security Requirements
State Agency/Entity - v 2019 01

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as "this Exhibit") sets forth the information security and privacy requirements the State Agency/Entity as defined by the State Administrative Manual (SAM) Section 4819.2 (hereinafter referred to as "State Entity") is obligated to follow with respect to all confidential and sensitive information (as defined herein) disclosed to or collected by State Entity, pursuant to State Entity's Agreement (the "Agreement") with the California Department of Social Services (hereinafter "CDSS") in which this Exhibit is incorporated. The CDSS and State Entity desire to protect the privacy and provide for the security of CDSS Confidential, Sensitive, and/or Personal (CSP) Information (hereinafter referred to as "CDSS CSP") in compliance with state and federal statutes, rules and regulations.

I. Order of Precedence. With respect to information security and privacy requirements for all CDSS CSP, unless specifically exempted, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between State Entity and CDSS.

II. Confidentiality of Information.

a. DEFINITIONS. The following definitions apply to this Exhibit and relate to CDSS Confidential, Sensitive, and/or Personal Information.

i. "Confidential Information" is information maintained by the CDSS that is exempt from disclosure under the provisions of the California Public Records Act (Government Codes Sections 6250 et seq.) or has restrictions on disclosure in accordance with other applicable state or federal laws.

ii. "Sensitive Information" is information maintained by the CDSS, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information is information in which the disclosure would jeopardize the integrity of the CDSS (i.e., CDSS' fiscal resources and operations).

iii. "Personal Information" is information, in any medium (paper, electronic, or oral) that identifies or describes an individual (i.e., name, social security number, driver's license, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information (PHI), etc.) and must be protected from inappropriate access, use or disclosure and must be made accessible to information subjects upon request. It can also be information in the possession of the Department in which the disclosure is limited by law or contractual Agreement (i.e., proprietary information, etc.).

iv. "Breach" is

1. the unauthorized acquisition, access, use, or disclosure of CDSS CSP in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

v. "Information Security Incident" is

1. unauthorized access or disclosure, modification or destruction of, or interference with, CDSS CSP that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of any state or federal law or in a manner not permitted under the Agreement between State Entity and CDSS, including this Exhibit.

b. CDSS CSP which may become available to State Entity as a result of the implementation of the Agreement shall be protected by State Entity from unauthorized access, use, and disclosure as described in this Exhibit.

c. State Entity is notified that unauthorized disclosure of CDSS CSP may be subject to civil and/or criminal penalties under state and federal law, including but not limited to:

- California Welfare and Institutions Code section 10850
- Information Practices Act - California Civil Code section 1798 et seq.
- Public Records Act - California Government Code section 6250 et seq.
- California Penal Code Section 502, 11140-11144, 13301-13303
- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") - 45 CFR Parts 160 and 164
- Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50
- Unemployment Insurance Code section 14013

d. EXCLUSIONS. "Confidential Information", "Sensitive Information", and "Personal Information" (CDSS CSP) does not include information that

i. is or becomes generally known or available to the public other than because of a breach by State Entity of these confidentiality provisions;

ii. already known to State Entity before receipt from CDSS without an obligation of confidentiality owed to CDSS;

iii. provided to State Entity from a third party except where State Entity knows, or reasonably should know, that the disclosure constitutes a breach of confidentiality or a wrongful or tortious act; or

iv. independently developed by State Entity without reference to the CDSS CSP.

III. State Entity Responsibilities.

a. Training. State Entity shall instruct all employees, agents, and subcontractors with access to the CDSS CSP regarding:

i. The confidential nature of the information;

ii. The civil and criminal sanctions against unauthorized access, use, or disclosure found in the California Civil Code Section 1798.55, Penal Code Section 502 and other state and federal laws; and

iii. CDSS procedures for reporting actual or suspected information security incidents in Paragraph IV - Information Security Incidents and/or Breaches.

b. Use Restrictions. State Entity shall take the appropriate steps to ensure that their employees, agents, and subcontractors will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes described in the Agreement and to meet its obligations under the Agreement.

c. Disclosure of CDSS CSP. State Entity shall not disclose any individually identifiable CDSS CSP to any person other than for the purposes described in the Agreement and to meet its obligations under the Agreement.

d. Subpoena. If State Entity receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CDSS CSP, State Entity will immediately notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer. In no event should notification to CDSS occur more than three (3) business days after receipt by State Entity's responsible unit for handling subpoenas and court orders.

e. Information Security Officer. State Entity shall designate an Information Security Officer to oversee its compliance with this Exhibit and to communicate with CDSS on matters concerning this Exhibit.

f. Requests for CDSS CSP by Third Parties. State Entity shall promptly transmit to the CDSS Program Contract Manager all requests for disclosure of any CDSS CSP, including Public Record Act (PRA) requests, (except from an Individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

g. Documentation of Disclosures for Requests for Accounting. State Entity shall maintain an accurate accounting of all requests for disclosure of CDSS CSP Information and the information necessary to respond to a request for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

h. Return or Destruction of CDSS CSP on Expiration or Termination. Upon expiration or termination of the Agreement between State Entity and CDSS, or upon a date mutually agreed upon by the Parties following expiration or termination, State Entity shall return or destroy the CDSS CSP. If return or destruction is not feasible, State Entity shall provide a written explanation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information in this Agreement. CDSS, in its sole discretion, will make a determination of the acceptability of the explanation and, if retention is permitted, shall inform State Entity in writing of any additional terms and conditions applicable to the retention of the CDSS CSP.

i. Retention Required by Law. If required by state or federal law, State Entity may retain, after expiration or termination, CDSS CSP for the time specified as necessary to comply with the law.

j. **Obligations Continue Until Return or Destruction**. State Entity's obligations regarding the confidentiality of CDSS CSP set forth in this Agreement, including but not limited to obligations related to responding to Public Records Act requests and subpoenas shall continue until State Entity returns or destroys the CDSS CSP or returns the CDSS CSP to CDSS; provided however, that on expiration or termination of the Agreement between State Entity and CDSS, State Entity shall not further use or disclose the CDSS CSP except as required by state or federal law.

k. **Notification of Election to Destroy CDSS CSP**. If State Entity elects to destroy the CDSS CSP, State Entity shall certify in writing, to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information, that the CDSS CSP has been destroyed.

l. **Personnel Management.** Before a member of State Entity's workforce may access CDSS CSP, State Entity agrees to implement personnel practices in compliance with SAM Section 5305.4 Personnel Management.

m. **Confidentiality Acknowledgement.** By executing this Agreement and signing Paragraph IX, CDSS Confidentiality and Security Compliance Statement, State Entity acknowledges that the information resources maintained by CDSS and provided to State Entity may be confidential, sensitive, and/or personal and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

n. **Confidentiality Safeguards.** State Entity shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the CDSS CSP that it creates, receives, maintains, uses, or transmits pursuant to the Agreement and SAM Section 5300. Including at a minimum the following safeguards:

    i. **Data Encryption.** All State Entity-owned or managed laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must be encrypted per SAM Section 5350.1 and using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). It is also recommended to encrypt other computing devices such as workstations or desktops.

    ii. **Data Transmission Encryption.** All data transmissions of CDSS CSP outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128 bit key or higher.

    iii. **Server Security.** Servers containing unencrypted CDSS CSP must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

    iv. **Removable Media Devices.** All electronic files that contain the CDSS CSP must be encrypted when stored on any removable media or portable device Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.

    v. **Minimum Necessary.** Only the minimum necessary amount of the CDSS CSP required to perform necessary business functions may be copied, downloaded, or exported.

vi. **Antivirus Software.** All State Entity-owned or managed workstations, laptops, tablets, and similar devices that process and/or store CDSS CSP must install and actively use comprehensive anti-virus software solution.

vii. **Patch Management.** To correct known security vulnerabilities, State Entity shall install security patches and updates in a timely manner on all State Entity-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP as appropriate based on State Entity's risk assessment of such patches and updates, the technical requirements of State Entity's systems, and the vendor's written recommendations. If patches and updates cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment.

viii. **Information Security Monitoring and Auditable Events.** For monitoring of its networks and other information assets, State Entity must comply with SAM Sections 5335 Information Security Monitoring and 5335.2 Auditable Events.

ix. **Paper Document Controls.** State Entity shall safeguard CDSS CSP in accordance with SAM Section 5365.2 Media Protection.

x. **Confidential Destruction**. CDSS CSP must be disposed of through confidential means, such as cross cut shredding and/or pulverizing.

IV. Information Security Incidents and/or Breaches of CDSS CSP

a. **CDSS CSP Information Security Incidents and/or Breaches Response Responsibility**. State Entity shall be responsible for facilitating the Information Security Incident and/or Breach response process as described in California Civil Code 1798.29(e) and SAM Section 5340, Information Security Incident Management, including, but not limited to, taking:

   i. Prompt corrective action to mitigate the risks or damages involved with the Information Security Incident and/or Breach and to protect the operating environment; and

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

b. **Discovery and Notification of Information Security Incidents and/or Breaches of CDSS CSP**. State Entity shall notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer of an Information Security Incident and/or Breach as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow State Entity to determine the scope of the Information Security Incident and/or Breach, but no later than three (3) calendar days after the discovery of an Information Security Incident and/or Breach. Notification is to be made by telephone call and email.

c. **Investigation of Information Security Incidents and/or Breaches**. State Entity shall promptly investigate such Information Security Incidents and/or Breaches of CDSS CSP. CDSS shall have the right to participate in the investigation of such Information Security Incidents and/or Breaches. CDSS shall also have the right to conduct its own independent investigation, and State Entity shall cooperate fully in such investigations. State Entity is not required to disclose their un-redacted confidential, proprietary, or privileged information. State Entity will keep CDSS fully informed of the results of any such investigation.

d. **Updates on Investigation**. State Entity shall provide regular (at least once a week) email updates on the progress of the Information Security Incident and/or Breach investigation of CDSS CSP to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer until the updates are no longer needed, as mutually agreed upon between State Entity and the CDSS Information Security and Privacy Officer. State Entity is not required to disclose their un-redacted confidential, proprietary, or privileged information.

e. **Written Report**. State Entity shall provide a written report of the investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within thirty (30) business days of the discovery of the Information Security Incident and/or Breach of CDSS CSP. State Entity is not required to disclose their un-redacted confidential, proprietary, or privileged information. The report shall include, but not be limited to, if known, the following:

    i. State Entity point of contact information;

    ii. A description of what happened, including the date of the Information Security Incident and/or Breach of CDSS CSP and the date of the discovery of the Information Security Incident and/or Breach, if known;

    iii. A description of the types of CDSS CSP that were involved and the extent of the information involved in the Information Security Incident and/or Breach;

    iv. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CDSS CSP;

    v. A description of where the CDSS CSP is believed to have been improperly transmitted, sent, or utilized;

    vi. A description of the probable causes of the improper use or disclosure;

    vii. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered; and

    viii. A full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Incident and/or Breach of CDSS CSP.

f. Cost of Investigation and Remediation. Per SAM Section 5305.8, State Entity shall be responsible for all direct and reasonable costs incurred by CDSS due to Information Security Incidents and/or Breaches of CDSS CSP resulting from State Entity's failure to perform or from negligent acts of its personnel, and resulting in the unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. These costs include, but are not limited to, notice and credit monitoring for twelve (12) months for impacted individuals, CDSS staff time, material costs, postage, media announcements, and other identifiable costs associated with the Information Security Incident, Breach and/or loss of data.

V. Contact Information. To direct communications to the above referenced CDSS staff, State Entity shall initiate contact as indicated herein. CDSS reserves the right to make changes to the contact information below by giving written notice to State Entity. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

CDSS Program Contract Manager	**CDSS** **Information Security & Privacy Officer**
See the Scope of Work exhibit for Program Contract Manager information	California Department of Social Services Information Security & Privacy Officer 744 P Street, MS 9-9-70 Sacramento, CA 95814 Email: iso@dss.ca.gov Telephone: (916) 651-5558

VI. Plan of Action and Milestones (POAM). The parties acknowledge that State Entity may have identified information security weaknesses or deficiencies where State Entity is not currently in full compliance with SAM and/or other applicable standards and/or requirements and, correspondingly, related provisions within this Exhibit. To the extent that those weaknesses or deficiencies have been identified and addressed by State Entity through the development of a POAM pursuant to SAM Section 5305.1, the development of the POAM and the progress towards remediation of weaknesses or deficiencies on the POAM shall be deemed to be compliance with the terms of this Exhibit.

VII. Amendment. The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CDSS CSP.

VIII. Interpretation. The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

IX. CDSS Confidentiality and Security Compliance Statement

CALIFORNIA DEPARTMENT of SOCIAL SERVICES
CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT v 2019 01

Information resources maintained by the California Department of Social Services (CDSS) and provided to your entity may be confidential, sensitive, and/or personal and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

We hereby acknowledge that the confidential and/or sensitive records of the CDSS are subject to strict confidentiality requirements imposed by state and federal law, which may include, but are not limited to, the following; the California Welfare and Institutions Code §10850, Information Practices Act - California Civil Code §1798 et seq., Public Records Act - California Government Code §6250 et seq., California Penal Code §502, 11140-11144, 13301-13303, Health Insurance Portability and Accountability Act of 1996 ("HIPAA") - 45 CFR Parts 160 and 164, and Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50. State Entity agrees to comply with the laws applicable to the CDSS CSP received.

This Confidentiality and Security Compliance Statement must be signed and returned with the Contract.

Project Representative

Name (Printed): _____

Title: _____

State Entity Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____

READ and ACKNOWLEDGED: Information Security Officer (or designee)

Name (Printed): _____

Title: _____

State Entity Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____

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

KIM JOHNSON
DIRECTOR

GAVIN NEWSOM
GOVERNOR

California Department of Social Services
Data De-Identification Reference Guide

I. Introduction

The California Department of Social Services (CDSS) is committed to providing useful data and promoting the transparency of state government through the public release of data. Prior to public release, all data must be assessed to determine whether any personal characteristics contained in the data pose the risk of identifying individuals. To protect the privacy of individuals served by the Department, the modified version of the Data De-Identification Guidelines (DDG)[1] developed by the California Health and Human Services Agency is being used.

Given that CDSS is not a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), the de-identification guidelines omit procedures mandated for HIPAA covered entities such as the expert determination process[2] and Safe Harbor[3]. This document describes the procedures that must be followed in preparing data for public release.

The CDSS procedures focus on the assessment of aggregate or summary data for purposes of de-identification and public release. Aggregate data is data that relates to a group or category of services or individuals. The aggregate data may be shown in table form as counts, percentages, rates, averages, or other statistical groupings.

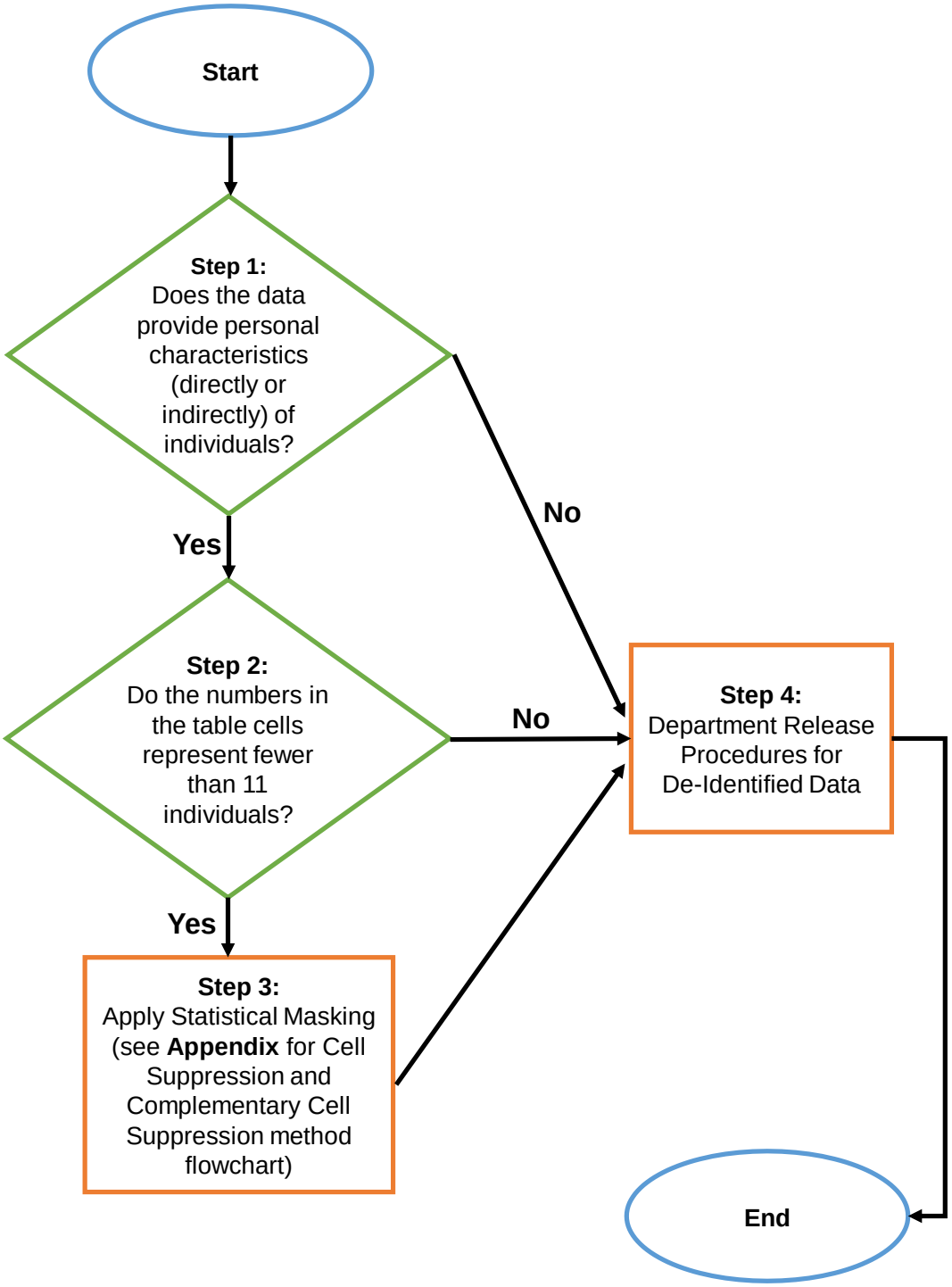
In contrast, record level data refers to a specific person or entity. Even after personal identifiers are removed, record level data inherently has higher risk than aggregate or summary data to identify an individual. Although the procedures should assist in reviewing record level data, a further case-by-case assessment must be made to ensure it is de-identified and does not include personal information that directly identifies an individual.

II. Data Assessment for Public Release Procedure

Prior to the public release of any CDSS data, the following four steps must be taken to ensure that any personal characteristics in the data cannot be used to identify an individual. While the examples below primarily focus on numbers presented in data tables, these steps also apply to any numbers or percent values present in written reports that represent fewer than 11 individuals.

[1] https://chhsdata.github.io/dataplaybook/resource_library/#datade-id
[2] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 41
[3] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 8

Flowchart of Steps for Data De-Identification



Step 1 – Personal Characteristics of Individuals

Does the data provide personal characteristics (directly or indirectly) that can be tied back to an individual?

Examples include but are not limited to: age, gender, race, ethnicity, language spoken, location of residence (including county), location of services received or accessed (including county), education status, financial status, physical description, sexual orientation, gender identity, medical history, and employment history.

If 'Yes', go to Step 2 – If 'No', go to Step 4.

Step 2 – Data Values (Table Cell Counts)

Do numbers in products such as tables and reports represent fewer than 11 individuals?

If 'Yes', go to Step 3 – If 'No', go to Step 4.

Step 3 – Statistical Masking

Which of the following statistical masking methods (Reduce Table Dimensions, Combine Categories, or Cell Suppression and Complementary Cell Suppression) will be used to de-identify the data?

Please keep in mind that multiple statistical masking methods may be used on the same set of data or within the same report.

Descriptions and examples of Step 3 are provided on pages 4 through 13. A flow chart of Step 3 is provided in the appendix on page 14.

After Completing Statistical Masking go to Step 4.

Step 4 – Departmental Release Procedures for De-Identified Data

What are the review and release procedures for the organization?

The expectation is that the review of data for de-identification will align with other routine review processes. Products containing de-identified data will undergo the standard data release approval process before public release, including any contractual obligations owed to the originators of the data. Products may include but are not limited to: reports, presentations, publications, tables, Public Records Act responses, media responses, and legislative responses.

Statistical Masking

Statistical Masking Method: Reduce Table Dimensions

A single table containing multiple column and row dimensions may have some cells that represent fewer than 11 individuals. This is seen in the unmasked version of *Example 1* below, which has two dimensions – *Education Level* and *Generation.* Producing multiple tables with fewer table dimensions can be used as a statistical masking method to increase the counts of individuals to at least 11. In the example below, the table dimensions *Education Level* and *Generation* are used to create two distinct tables, which increases the numbers within each table cell to represent at least 11 individuals.

Example 1: Reduced Table Dimensions
Unmasked – Education Level by Generation

Generation	High School Diploma/GED	Associates	Bachelors	Graduate	Total
Millennial (18-34)	134	150	78	8	370
Generation X (35-50)	371	237	50	3	661
Total	505	387	128	11	1031

Masked -Generation

Generation	Total
Millennial (18-34)	370
Generation X (35-50)	661
Total	1031

Masked - Education Level

Education Level	Total
High School Diploma/GED	505
Associates	387
Bachelors	128
Graduate	11
Total	1031

Statistical Masking Method: Combine Categories

Combining multiple categories into a single category may increase the value of a table cell to a number representing at least 11 individuals, as in the example below, in which multiple ethnic groups are combined into a single "Other" category.

Example 2: Combine Categories
Unmasked – Services Accessed by Ethnicity

Service Type	Black	White	Latino	Asian	Native American	Other	Total
Substance Abuse Service	40	208	88	4	3	37	380
Mental Health Service	28	237	79	11	8	19	382
Total	68	445	167	15	11	56	762

Masked – Ethnicity

Service Type	Black	White	Latino	Other	Total
Substance Abuse Service	40	208	88	44	380
Mental Health Service	28	237	79	38	382
Total	68	445	167	82	762

In *Example 2 Asian*, *Native American*, and *Other*, will be merged into a single *Other* category. Creating a single *Other* category will ensure that no cells represent fewer than 11 individuals. The advantage of combining categories is the ability to present two data elements, such as ethnicity and service type, in a single table.

The ethnicity categories *Asian* and *Native American* were selected to be combined because they contain the smallest values. After combining the *Asian* and *Native American* categories, however, the number of individuals accessing *Substance Abuse* services still represents fewer than 11 individuals. Since the category *Other* provides less granular information than *Black*, *White*, or *Latino*, which designate specific ethnic groups, *Other* will be combined with *Asian* and *Native American* to ensure that the new *Other* category contains numbers that represent at least 11 individuals.

Note: Footnotes should be used to indicate which categories have been combined.

Statistical Masking Method: Cell Suppression and Complementary Cell Suppression

If reducing table dimensions or combining categories is not practical, then it may be necessary to suppress all cells that represent fewer than 11 individuals. Complementary cells, which are cells that could be used to calculate and re-identify suppressed cells (i.e., cells representing fewer than 11 individuals), will also need to be suppressed. This masking method might be selected if the report requires a greater level of detail, such as a county-based report.

When suppressing values, the following footnote is recommended to indicate the suppression:

- "Values are not visible to protect the confidentiality of the individuals summarized in the data."[4]

How to Suppress Small Cells and Perform Complementary Cell Suppression:

1: Suppress Small Cells

Small Cells: Cells that represents fewer than 11 individuals.

- Mask all numbers (cell values) that are less than 11 (i.e., derived from fewer than 11 individuals) with an asterisk (*), when possible.
    - Note: Values of zero (0) are typically shown since a non-event cannot be identified[5].
- If a complementary cell must be suppressed and has a value of 11 or greater, a double asterisk (**) should be used, whenever possible, to differentiate it from cells suppressed with a value of less than 11.

Example 3: Small Cell Suppression Unmasked – Application Approvals by Family Type

Applications	Single Parent	Two Parent
Approved	56	15
Denied	5	0
Pending	12	6

Masked Application Approvals by Family Type

Applications	Single Parent	Two Parent
Approved	56	15
Denied	*	0
Pending	12	*

[4] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 39
[5] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 15

2: Complementary Cell Suppression

Complementary Cell: A number representing more than 11 individuals that can be used to calculate and re-identify a small cell or small cells.

Complementary Cell Suppression: When a number representing 11 or more individuals is suppressed using one of the methods listed below to prevent the re-identification of other suppressed cells.

- Numbers 11 and higher may need to be suppressed (i.e., complementary cell suppression) if any numbers less than 11 can be re-identified through the addition or subtraction of any unsuppressed numbers. When numbers 11 and higher are suppressed, a double asterisk should be used whenever possible.
- In each column or row containing a suppressed number, at least one other number must be suppressed through complementary cell suppression[6].
- In cross tables (tables containing both column and row totals), if a number is suppressed then both the column and row must be checked to determine if complementary cell suppression is necessary.

***Methods of Complementary Suppression*[7]:**

One of the following methods should be selected for use. The composition of the data or specific reporting needs of the organization may be used to determine which of the following four options will be used.

- Next Smallest Number:
  - Suppress the next smallest unsuppressed number. This method retains larger numbers that represent more individuals (see *Example 4 – Option A* on page 8).
    Note: There is no maximum value of the "Next Smallest Number."

- Suppress/Roll-up Total:
  - Suppress the number containing the row or column sum. This method allows for automation of the suppression process (i.e., through the use of Excel macros and formulas), which reduces human error (see *Example 4 – Option B* on page 9).

- 'Least Interesting' Category:
  Suppress the 'least interesting' category. This is often a category such as 'other' or 'I don't know' (see *Example 4 – Option C* on page 10).

[6] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 19
[7] Data De-Identification Guidelines (DDG), California Health and Human Services, Version 1.0 (2016), p. 20

- Similar Group:
  - Suppress the cell most similar to the cell needing complementary suppression, such as adjacent age groups. This can produce complementary suppression that may be easier to interpret (see *Example 4 – Option D* on page 10).

Example 4: Complementary Cell Suppression
Unmasked – Barriers to Housing

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	1	12	13	2,765
White	3,732	1,465	9	16	22	5,244
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

1: Suppress Small Cells

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	*	12	13	2,765
White	3,732	1,465	*	16	22	5,244
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

2: Complementary Cell Suppression

Option A – Next Smallest Number

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	*	**	13	2,765
White	3,732	1,465	*	**	22	5,244
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

In the previous table, the next smallest number was suppressed where it would be possible to re-identify a suppressed small cell (see highlighted cells). The examples below demonstrate how cells can be re-identified by subtracting all unsuppressed cells from the total, if complementary cell suppression does not occur.

Black: 1 – Total *Black* individuals with *Criminal Record (Self)* as a barrier to housing

$$\begin{array}{r} 2{,}765 \\ 1{,}561 \\ 1{,}178 \\ 12 \\ -\quad 13 \\ \hline 1 \end{array}$$

White: 9 – Total *White* individuals with *Criminal Record (Self)* as a barrier to housing

$$\begin{array}{r} 5{,}244 \\ 3{,}732 \\ 1{,}465 \\ 16 \\ -\quad 22 \\ \hline 9 \end{array}$$

2: Complementary Cell Suppression

Option B – Suppress/Roll-up Total

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	*	12	13	**
White	3,732	1,465	*	16	22	**
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

Instead of suppressing the next smallest number, the total column can be suppressed or rolled up to prevent the re-identification of small cells. Because the total column is suppressed, one cannot use the total to calculate the suppressed numbers in the *Criminal Record (Self)* cells.

2: Complementary Cell Suppression

Option C – 'Least Interesting' Category

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	*	12	**	2,765
White	3,732	1,465	*	16	**	5,244
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

The table above demonstrates complementary cell suppression in which the 'least interesting' category is suppressed. *Other* is the 'least interesting' category, since it is not a specific barrier to housing like the other categories

2: Complementary Cell Suppression

Option D – Similar Group

Ethnicity	Poor Credit	Past Evictions	Criminal Record (Self)	Criminal Record (Family Member)	Other	Total
Black	1,561	1,178	*	**	13	2,765
White	3,732	1,465	*	**	22	5,244
Latino	4,028	1,227	13	15	15	5,298
Other	4,929	1,510	11	19	17	6,486

Complementary cell suppression in the table above is accomplished by suppressing the group with characteristics most similar to the category requiring small cell suppression. Since *Criminal Record (Self)* is suppressed due to small cell size, the category which represents a group with similar characteristics, *Criminal Record (Family Member)*, is selected for complementary cell suppression. Coincidentally, the tables produced by suppressing the next smallest number (Option A) and a similar group (Option D) are the same in this example. This may not always be the case with all data.

Important Data Issues to Consider:

Complementary Cell Suppression for Cells with Identical Data

In a row containing two suppressed cells, the numbers contained in the suppressed cells typically cannot be re-identified by subtracting the unsuppressed cells from the total. When each suppressed cell equals one, however, it is possible to re-identify the number in each suppressed cell if the total cell is not suppressed. In *Example 5*, the next smallest number is suppressed during complementary cell suppression to prevent the cells containing the number of infants in a Group Home or Guardian placement from being re-identified.

Example 5: Complementary Cell Suppression

Unmasked – Infant Placement Types

Infants (Under 1)	Foster Care	Group Home	Guardian	Other	Total
Count	1,178	1	1	18	1,198

1: Suppress Small Cells

Infants (Under 1)	Foster Care	Group Home	Guardian	Other	Total
Count	1,178	*	*	18	1,198

2: Complementary Cell Suppression (Next Smallest Number)

Infants (Under 1)	Foster Care	Group Home	Guardian	Other	Total
Count	1,178	*	*	**	1,198

Even when a row or column has at least two numbers suppressed, it may still be possible to re-identify a suppressed number. In this case, all numbers that can be used to re-identify a suppressed number must be masked.

Complementary Cell Suppression with Multiple Cells Containing Zeros

In *Example 6*, the column containing the count for each family size group has one suppressed row, the *1 to 2 children* category. All other rows contain zeros. Because the column total reflects the value of the suppressed cell, the column total is also suppressed. This suppression results in a table in which the only visible values are zeroes. It is important to remember, however, that zeroes are important pieces of data that can convey meaningful information.

Example 6: Complementary Cell Suppression

Unmasked – Family Size (Small County)

Family Size	Count
1 to 2 children	1
3 to 4 children	0
5 to 6 children	0
6+ children	0
Total	1

Suppress Small Cells

Family Size	Count
1 to 2 children	*
3 to 4 children	0
5 to 6 children	0
6+ children	0
Total	*

Cell Suppression of Numbers in Text

Cell suppression guidelines also apply to any numbers that are included in the body of a report or other written document.

Numbers representing fewer than 11 individuals are unsuppressed in the report text below, which goes against the de-identification guidelines.

> **Sample Sentence:**
> "Out of 35 children, 6 were in care for 12 to 23 months and 5 were in care for 24 to 35 months"

This can be corrected by combining the two time-in-care categories into either a single category:

> **Sentence Revised for Suppression:**
> **"**Out of 35 children, 11 were in care for 12 to 35 months."

Or by using asterisks or text to suppress numbers representing fewer than 11 individuals:

> **Sentence Revised for Suppression:**
> "Out of 35 children, fewer than 11 were in care for 12 to 23 months and fewer than 11 were in care for 24 to 35 months"

Cell Suppression of Percentages in Text

Cell suppression guidelines apply to any reports or tables containing percentages. Percent values of small cells or complementary cells which could be used to re-identify masked numbers also need to be suppressed.

Because it is possible to determine the number of children in each group by multiplying the percent values against the total number of children [6 children were in care for 12 to 23 months (35 × 0.17 = 5.95) and 5 children were in care for 24 to 35 months (35 × 0.14 = 4.9)] the percent values must also be suppressed.

Sample Sentence:
"Out of 35 children, 17% were in care for 12 to 23 months and 14% were in care for 24 to 35 months"

This can be corrected by combining the two time in care categories into a single category:

Sentence Revised for Suppression:
"Out of 35 children, 31% were in care for 12 to 35 months."

Or by using asterisks or text to suppress numbers representing fewer than 11 individuals:

Sentence Revised for Suppression:
"Out of 35 children, *% were in care for 12 to 23 months and *% were in care for 24 to 35 months."

Small Numbers Not Representing Individuals

Small numbers do not need to be suppressed if they do not represent individuals. In *Example 7*, the number 9 does not need to be suppressed because it shows the difference between the cases carried forward from last month and the total from last month's report (i.e., 6,454 - 6,445 = 9), not 9 individuals.

Example 7: Small Numbers Not Representing Individuals

Caseloads	Two Parent Families
Cases carried forward from last month	6,454
Total from last month's report	6,445
Adjustment (difference between rows)	9

Appendix: Cell Suppression and Complementary Cell Suppression Flowchart