MEMORANDUM OF UNDERSTANDING
BETWEEN
THE CALIFORNIA STATEWIDE AUTOMATED WELFARE SYSTEM CONSORTIUM
AND
CHILD WELFARE DIGITAL SERVICES

This MEMORANDUM OF UNDERSTANDING (MOU) is entered between the California Statewide Automated Welfare System (CalSAWS) Consortium and Child Welfare Digital Services (CWDS), a Division of CalHHS's Office of Technology and Solutions Integration. CWDS is operating on behalf of and due to delegated authority to operate on this MOU by California Department of Social Services (CDSS) for the Child Welfare Services - California Automated Response and Engagement System (CWS-CARES). For the remainder of the document "party" refers to either of the two entities – CWDS or the CalSAWS Consortium and "parties" refers to both CWDS and the CalSAWS Consortium.

A. PURPOSE

This MOU establishes a collaborative framework between the parties for the secure, compliant, and efficient exchange of client data. The purpose of this data exchange is to support joint programmatic, operational, and analytical functions that enhance service delivery, benefits coordination, and child welfare outcomes.

This MOU is executed in alignment with the federal regulatory requirements governing Comprehensive Child Welfare Information Systems (CCWIS), specifically 45 CFR §1355.52, which mandates that a CCWIS system must:

- Maintain all program data required by federal, state, or tribal law or policy.
- Support bi-directional data exchanges with external systems as specified in §1355.52(e).
- Ensure data quality and integrity as required under §1355.52(d).
- Apply appropriate data exchange standards per §1355.52(f).

The CalSAWS and CWS-CARES systems support critical business functions that automate foster care eligibility determinations and reduce reliance on manual data entry between systems. This automation improves data accuracy, enhances the ability to generate timely and reliable statistics, and reduces the volume of inquiries directed at the CalSAWS Consortium and CWS-CARES staff by enabling more efficient and accurate data sharing.

B. RECITALS

CWS-CARES is a cloud-based system being developed to replace California's legacy child welfare IT systems. It is designed to support child welfare professionals by enhancing case management, data sharing, and service delivery for children and families involved in the child welfare system. CWS-CARES is being developed in alignment with federal requirements under Title IV-E of the Social Security Act,

which governs funding and standards for child welfare services, including the implementation of CCWIS.

The CalSAWS Consortium was established as a Joint Powers Authority (JPA) through a collective agreement with all 58 of California's county welfare departments. This JPA serves as a single legal entity responsible for managing the CalSAWS system, which maintains client data for the counties. Such client data is considered confidential under Welfare and Institutions Code (WIC) §10850 and must be protected from unauthorized access in accordance with state and federal laws.

WIC Section 10850 authorizes any county welfare department in the state to provide lists of applicants for, or recipients of, public social services, to other county welfare departments or to CDSS. These records may be released upon request by CDSS and must be used solely for purposes directly connected with the administration of public social services. The report required pursuant to § 55 of Chapter 47 of the Statutes of 2012 (Senate Bill 1041) is considered directly connected with such administration.

CalSAWS and CWS-CARES are enterprise systems that support distinct but complementary functions within California's health and human services programs. CalSAWS facilitates eligibility and enrollment for public assistance programs, while CWS-CARES supports case management for child welfare services. Both systems are integral to automating foster care eligibility determinations, reducing manual data entry, improving data accuracy, and enhancing the ability to generate reports and respond to child welfare needs efficiently.

The parties recognize that secure, bi-directional data exchange between the CalSAWS and CWS-CARES systems will reduce duplicative data entry, streamline workflows, and minimize the volume of inquiries to staff by enabling timely, accurate, and automated data sharing.

This MOU is intended to align with the federal regulatory requirements governing CCWIS, specifically 45 CFR §1355.52, which mandates support for external data exchanges, data quality, and the use of standardized data exchange protocols.

Now, therefore, the parties enter this MOU to formalize their mutual understanding and responsibilities regarding the exchange of client data between CalSAWS and CWS-CARES.

C. TERMS

1. This MOU governs the exchange of client data between CalSAWS and CWS-CARES systems to support eligibility determinations, benefits coordination, and child-welfare-related functions.
2. The interface specification documents for CWS-CARES developed by CWDS in collaboration with CalSAWS define the specific data fields exchanged under this MOU – these are located on the CalSAWS Project Sharepoint Site. The parties agree to jointly maintain and version-control these specifications to ensure traceability. Updates to the Data Elements List do not require amendments to his MOU, provided the overall data classification remains unchanged. Any changes to

the data elements list will be documented and communicated through the established change control process. If any change elevates the risk classification beyond the current classification or introduces new statutory implications, the parties agree to initiate a formal review and consider amending this MOU.

3. The parties agree to implement and maintain appropriate security controls to protect shared systems and data. Each party shall adhere to the following requirements, which are equally applicable to both entities and are further supported by applicable State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), and CDSS Confidentiality and Security Requirements documents. The specific communication protocols, data elements, and transaction-level requirements for each interface will be defined in the Interface System Design (ISD) document. All interface designs must conform to the security objective described in SAM and SIMM. In the event of any conflict between applicable requirements, the more stringent or higher control shall prevail.

    i. Abide by CWS-CARES service account management requirements, including key rotation, secret management, password complexity, multi-factor authentication (MFA), and least privilege access, as defined by CWDS project security controls and State Policy.
    ii. Apply appropriate levels of confidentiality, integrity, and availability to CWS-CARES data, in accordance with data classification, FIPS Publication 199 protection levels, and the SAM.
    iii. Conform to State standards for secure data transmission and storage, including encryption and destruction practices based on data classification.
    iv. Comply with all applicable statewide policies and laws regarding the use and protection of information resources and data, including those set forth in the SAM.
    v. Enforce least privilege and need-to-know principles for data access.
    vi. Ensure all systems communicating with CWDS are regularly patched, upgraded, and protected with current antivirus software.
    vii. Promptly notify CWDS ISO of any security incidents involving shared systems or data by contacting CWDSinfosec@otsi.ca.gov.
    viii. Engage the CWS-CARES data owner in any investigation of a security incident involving CWS-CARES data, the service account, or the interface, and cooperate fully as data custodians.
    ix. Maintain responsibility for acceptable use of any system accounts that have been provisioned and prevent disclosure or misuse, in accordance with State Policy.
    x. Acknowledge the CWDS' right to disable or remove service accounts deemed a security risk by the CWDS ISO.
    xi. Annually attest to the continued need for the interface and associated data exchange.
    xii. Immediately notify CWSCARESInterfaces@otsi.ca.gov of any changes to the business need for the interface, the classification of data being exchanged, or the details of the credential request, including organizational points of contact.

4. Both parties acknowledge that the security controls for this exchange are based on the Data Classification and related NIST requirements for securing data. Data Classification is based on sensitivity, regulatory impact, and operational dependency. The CWS-CARES system base classification is Moderate. The parties agree that if data elements

are added, removed, or modified this MOU will remain valid and enforceable without requiring additional approval or amendment. If any change elevates the risk classification beyond the current classification or introduces new statutory implications, the parties agree to initiate a formal review and consider amending the MOU. The parties agree to transmit data using secure methods such as API endpoints, encrypted file transfer protocols (SFTP), or other mutually agreed secure channels. The exchange may occur on a daily, weekly, or event-driven basis, as defined in the technical implementation guide. Data formats will include JSON, XML, or CSV, with schema definitions maintained in a shared repository accessible to both parties. The CalSAWS Consortium agrees to work cooperatively with CWDS, if needed, by providing clarifications of the client data sent to CWS-CARES and/or identifying and assessing additional client data maintained by CalSAWS that may be relevant and necessary for the completion of the evaluation and report mandated by the Legislature.

5. Each party agrees to comply with all applicable federal and state laws and regulations, including but not limited to HIPAA, FERPA, and California Civil Code §1798. Data will be used solely for authorized purposes and protected against unauthorized access, disclosure, or misuse. The parties agree to implement and maintain administrative, technical, and physical safeguards to ensure data confidentiality, integrity, and availability.
6. In the event of a data breach or unauthorized access, the affected party agrees to notify the other within 24 hours of discovery. Notification should also be sent via email to CWDSinfosec@otsi.ca.gov. Both parties will promptly meet and confer regarding the scope and parameters of a joint investigation, including how to coordinate and effectuate remediation efforts. For any joint investigation, post-incident reviews and corrective actions will be documented and shared to ensure transparency and continuous improvement. Nothing in this section shall be construed as a requirement to share confidential and/or proprietary information regarding security and/or information systems.
7. The MOU may be amended by mutual written agreement between the parties.

D. CONTACTS

1. The following CWDS representative is authorized to implement the terms and conditions of the MOU and will be responsible for the oversight and supervision of the security and confidentiality of the client data sent to CWS-CARES system by CalSAWS system:

   Kimberly Glenn, Assistant Deputy Director, CWDS
   2870 Gateway Oaks Drive
   Sacramento, CA 95833
   (916) 653-1428
   kimberly.glenn@otsi.ca.gov

   CWDS will immediately notify the CalSAWS Consortium Executive Director, in writing, of a change of the contact person.

2. The following CalSAWS Consortium representative is authorized to implement the terms and conditions of the MOU and will be responsible for the oversight and supervision of the security and confidentiality of the transmission of client data sent by the CalSAWS system to the CWS-CARES system:

   Julia Erdkamp, Executive Director, CalSAWS
   11971 Foundation Place
   Gold River, CA 95670
   (916) 282-3549
   erdkampJ@CalSAWS.org

   CalSAWS will immediately notify the CWS-CARES Assistant Deputy Director, in writing, of a change of the contact person.

E. TERM

The MOU shall be effective upon the signing of the authorized representatives of the parties. This MOU shall remain in effect from the effective Date and shall continue in force so long as CWS-CARES and/or CalSAWS remain active systems and maintain connectivity through the interface described herein, unless amended or terminated by mutual agreement.

F. FUNDING

There is no funding or fiscal reimbursement for the provision of the client data pursuant to this MOU.

G. AUTHORIZED REPRESENTATIVES

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

THE PARTIES HERETO have executed this MOU:

Child Welfare Digital Services
Cynthia Tocher, Deputy Director, CWDS

Signature: DocuSigned by: Cynthia Tocher F4000980CC4E449... **Date:** 3/23/2026
Deputy Director, CWDS

CalSAWS
Michael Sylvester, Consortium Chair, CalSAWS

Signature:_____ **Date:**_____
CalSAWS Consortium Chair

Julia Erdkamp, Executive Director, CalSAWS

Signature:_____ **Date:**_____
CalSAWS Executive Director

Approved as to legal form:

Signature:_____ **Date:**_____
Kronick Moskovitz Tiedemann & Girard,
Consortium Legal Counsel

APPENDICES

The following appendices are incorporated into this MOU and provide supporting details referenced in the main body of the agreement.

Appendix A – Definition of Key Terms

This appendix defines key terms used throughout the MOU to ensure mutual understanding and consistency.

- **External Systems:** In the context of child welfare and aligned with CCWIS requirements, external systems are information systems operated by entities outside the title IV-E agency that exchange data with the CCWIS. These may include systems operated by courts, education agencies, health providers, or other service organizations. External systems are not part of the CCWIS but must comply with applicable data exchange, security, and interoperability standards
- **Program Data**: refers to any information that are required to support the administration, management, and oversight of child welfare programs (e.g., case management, financial, provider, administrative, for federal reporting, and data shared/received from external systems).

Appendix B - CDSS Confidentiality and Security Requirements

This appendix provides detailed list of the specific SAM and SIMM requirements that correspond to the security controls outlines in Section C, item 3 of this MOU, to ensure clarity and alignment with statewide standards.

The State of California uses the NIST 800-53, Rev 5 as the control baseline for systems. The CISA Zero-Trust framework and the FIPS 140-3 are required standards.

1. **Service Account Management**
   - SAM 5360 – Identity and Access Management
   - SAM 5305.3 – Information Security Roles and Responsibilities
   - SAM 5335.1 – Continuous Monitoring
   - SIMM 5360-C – Multi-Factor Authentication

2. **Data Confidentiality, Integrity, and Availability**
   - SAM 5300.2 – Information Security Program Requirements
   - SAM 5305.5 – Information Asset Management
   - SAM 5305.6 – Risk Management
   - SAM 5305.7 – Risk Assessment
   - SAM 5310.4 – Individual Access to Personal Information
   - SAM 5310.5 – Information Integrity
   - FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems

3. **Data Transmission, Storage, and Destruction**

- SAM 5310.6 – Data Retention and Destruction
- SAM 5350.1 – Encryption
- SAM 5355 – Endpoint Defense
- SAM 5365.3 – Media Disposal
- SIMM 5355-A – Endpoint Protection Standard
- SIMM 5360-A – Telework and Remote Access Security Standard

4. **Compliance with Statewide Policies**
   - SAM 5300.5 – Minimum Security Controls
   - SAM 5305 – Information Security Program
   - SAM 5305.8 – Provisions for Agreements with State and Non-State Entities
   - SAM 5310.7 – Security Safeguards
   - SAM 5350 – Operational Security
   - SIMM 140 – Cloud Security Guide
   - SIMM 5305-A – Information Security Program Management Standard
   - SIMM 5330-H – Information Security Policy Compliance and Enforcement Standard
   - SIMM 5350-A – Zero Trust Architecture Standard

5. **Least Privilege and Need-to-Know**
   - SAM 5310 – Privacy
   - SAM 5310.2 – Limiting Collection
   - SAM 5310.3 – Limiting Use and Disclosure
   - SAM 5310.8 – Privacy Threshold and Privacy Impact Assessments
   - SAM 5315.6 – Activate Only Essential Functionality
   - SIMM 5310-A – Privacy Statement and Notices Standard

6. **System Maintenance and Protection**
   - SAM 5315.2 – System Development Lifecycle
   - SAM 5315.5 – Configuration Management
   - SAM 5355.1 – Malicious Code Protection
   - SIMM 5345-A – Vulnerability Management Standard
   - SIMM 5355-B – Server Hardening Policy

7. **Incident Notification and Response**
   - SAM 5325 – Business Continuity with Technology Recovery
   - SAM 5325.6 – Information System Backups
   - SAM 5330.2 – Compliance Reporting
   - SAM 5340 – Incident Security Incident Management
   - SAM 5340.3 – Incident Handling
   - SAM 5340.4 – Incident Reporting
   - SIMM 5325-A – Technology Recovery Plan Instructions
   - SIMM 5335-A – Security Event Notification and Response Standard
   - SIMM 5340-A – Incident Reporting and Response Instructions
   - SIMM 5340-C – Requirements to Respond to Incidents Involving a Breach of Personal Information

8. **Interface Review and Attestation**

- SAM 5315.8 – Information Asset Connections
- SIMM 5330-B – Information Security and Privacy Program Compliance Certification
- SIMM 5330-F – Information Security and Privacy Compliance and Enforcement Standard