MEMORANDUM OF UNDERSTANDING
BETWEEN
THE CALIFORNIA STATEWIDE AUTOMATED WELFARE SYSTEM CONSORTIUM
AND
CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION/CALIFONIA CORRECTIONAL HEALTH CARE SERVICES

This MEMORANDUM OF UNDERSTANDING (MOU) is entered between the California Statewide Automated Welfare System (CalSAWS) Consortium and the California Department of Corrections and Rehabilitation (CDCR)/California Correctional Health Care Services (CCHCS). For the remainder of the document "party" refers to either of the two entities – CDCR/CCHCS or the CalSAWS Consortium and "parties" refers to both CDCR/CCHCS and the CalSAWS Consortium.

A. PURPOSE

This MOU establishes a collaborative framework between the parties for the secure, compliant, and efficient exchange of Medi-Cal Personally Identifiable Information (Medi-Cal PII). The purpose of this data exchange is to support joint programmatic, operational, and analytical functions that enhance service delivery, benefits coordination, and health care services for justice-involved individuals.

This MOU is executed in alignment with state and federal regulatory requirements governing Medi-Cal PII. Specifically, this MOU is established in compliance with section 14100.2 of the Welfare and Institutions Code (W&I Code) and section 431.302 of Title 42 of the Code of Federal Regulations (CFR), which mandate that Medi-Cal PII may only be used and disclosed to assist in the administration of Medi-Cal.

Since 2014, California Department of Health Care Services (DHCS) and CDCR have had processes in place to support Transitional Case Management Program (TCMP) benefit workers with assisting all eligible incarcerated individuals, who are released to Parole or Post Release Community Supervision, with Medi-Cal application assistance approximately 90-135 days prior to release from a California state correctional institution (ACWDL 24-04). As part of that enrollment process and to support the suspension of benefits processes, CDCR TCMP benefit workers report release dates for individuals being released from CDCR custody to the county agency where their Medi-Cal is established. County eligibility workers then use the release date to activate the member's benefits upon their release from incarceration.

The CalSAWS and CDCR/CCHCS systems support critical business functions that automate communication between TCMP benefit workers and the county departments/agencies statewide and reduce reliance on manual data entry of release date information for incarcerated individuals. This approach contributes to establishing a continuum of care between CDCR/CCHCS and the community, ultimately allowing justice-involved populations access to vital medical and

behavioral health services upon their release.

B. RECITALS

The CalSAWS Consortium was established as a Joint Powers Authority (JPA) through a collective agreement between all 58 of California's counties.. This JPA serves as a single legal entity responsible for managing the CalSAWS system, which maintains client data for the counties, including Medi-Cal PII. Medi-Cal PII may be used or disclosed only for purposes directly connected to the administration of Medi-Cal, in accordance with Welfare and Institutions Code section 14100.2, 42 CFR section 431.302, and all applicable state and federal privacy and security requirements.

Under the CalAIM Justice-Involved Reentry Initiative, and Welfare and Institutions Code Section 14184.800, CDCR provides 90-day pre-release Medi-Cal services and care-coordination for eligible incarcerated individuals prior to their release. Administering this program necessitates timely data sharing and the implementation of Medi-Cal pre-release application and suspension processes with counties. CDCR supports those application processes for eligible incarcerated individuals through TCMP. These activities include submitting pre-release Medi-Cal applications and reporting release-date information to the county departments/agencies responsible for the individual's Medi-Cal case. Counties rely on this information to carry out Medi-Cal benefits suspension and activation requirements under Welfare and Institutions Code § 14011.10 and 14011.11.

CalSAWS and CDCR/CCHCS each perform essential functions in supporting Medi-Cal eligibility, suspension, and activation for justice-involved individuals. Current processes require manual data entry and multiple handoffs between systems, which can delay county actions and increase administrative workload. Both parties recognize that a secure, automated bi-directional data exchange will improve accuracy, timelines, and efficiency in transmitting release-date information and other relevant updates to support Medi-Cal eligibility operations per ACWDL 24-04.

This MOU aligns with federal Medicaid requirements governing the confidentiality, use, and exchange of Medicaid information, including 42 CFR sections 431.300-431.307 and 42 CFR sections 435.940–435.965.

Now, therefore, the parties enter into this MOU to formalize their mutual understanding and responsibilities regarding the exchange of client data between CalSAWS and CDCR/CCHCS.

C. TERMS

1. This MOU governs the exchange of Medi-Cal PII between CalSAWS and CDCR/CCHCS systems to support automation of reporting release dates and other member updates to counties as required to support the suspension of benefits processes for incarcerated Medi-Cal members, per ACWDL 24-04.

2. CDCR/CCHCS and CalSAWS will interface specific data fields exchanged under this MOU as follows:

- **CDCR/CCHCS to CalSAWS Data Fields:** CDCR Patient ID, Controlling CDCR Number, CDCR Admission Date, First Name, Last Name, Date of Birth (DOB), Gender, Social Security Number (SSN), Client Index Number (CIN), CDCR Institution, Estimated Release Date, Actual Release Date, County of Release, Change Type

- **CalSAWS to CDCR/CCHCS Data Fields:** CDCR Patient ID, First Name, Last Name, Date of Birth (DOB), Gender, Social Security Number (SSN), Client Index Number (CIN), Known to CalSAWS, Medi-Cal Program Status, Medi-Cal Effective Date, Address Line 1, Address Line 2, City, State Code, County Code, Zip Code,

Updates to the Data Fields Lists 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 by DHCS, in partnership with CDCR/CCHCS, to CalSAWS following existing processes. 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 Medi-Cal PII. 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 DHCS 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 DHCS service account management requirements, including key rotation, secret management, password complexity, multi-factor authentication (MFA), and least privilege access, as defined by DHCS project security controls and State Policy.
    ii. Apply appropriate levels of confidentiality, integrity, and availability to Medi-Cal PII, 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 CalSAWS are regularly patched, upgraded, and protected with current antivirus software.
    vii. Promptly notify DHCS ISO of any security incidents involving shared systems or data by contacting xxx.

viii. Engage the Medi-Cal PII owner in any investigation of a security incident involving Medi-Cal PII, the service account, or the interface, and cooperate fully as data custodians.
ix. Annually attest to the continued need for the interface and associated data exchange.
x. Immediately notify CalSAWS and CDCR/CCHCS 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 CDCR/CCHCS 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, consistent with security protocols existing at the time of the added data elements per SAM, SIMM, or NIST. 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 and CDCR/CCHCS agree to work cooperatively, if needed, by providing clarifications of the client data sent to CalSAWS and/or identifying and assessing additional client data maintained by CDCR/CCHCS 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, CMIA, and Information Practices Act of 1977 (California Civil Code §1798). Each party shall use data solely for authorized purposes and shall protect such data from unauthorized access, disclosure, or misuse. The parties further agree to implement and maintain appropriate administrative, technical, and physical safeguards to ensure confidentiality, integrity, and availability of the data.

6. In the event of a data breach or unauthorized access, the affected party shall notify the other party without unreasonable delay, and in no event later than 24 hours after discovery. Such notification should be sent via email to Security.Officer@CalSAWS.org and CCHCS-ISO@cdcr.ca.gov.

7. Following any incident or suspected breach, the parties shall promptly meet and confer regarding the scope, nature, and impact of the incident, including coordination of a joint investigation and any necessary mitigation/ remediation efforts. Any joint investigation, post-incident reviews and corrective actions shall be appropriately documented and shared between the parties to promote transparency and continuous improvement. Nothing in this section shall be construed to require either party to disclose or share confidential proprietary, /or security- sensitive information including security measures and/or information systems.

DRAFT

8. The MOU may be amended by mutual written agreement between the parties.

D. CONTACTS

1. The following CDCR/CCHCS 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 the CDCR/CCHCS system by CalSAWS system:

   Monica Campos, Manager II, CDCR/CCHCS
   8280 Longleaf Dr.
   Elk Grove, CA 95758
   (916) 691-2855
   Monica.Campos@cdcr.ca.gov

   CDCR/CCHCS 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 CDCR system:

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

   CalSAWS will immediately notify the CDCR/CCHCS contact, Monica Campos, 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 CDCR/CCHCS 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 Medi-Cal PII pursuant to this MOU.

DRAFT

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:

California Department of Corrections and Rehabilitation

Signature:_____ **Date:**_____
Lara Saich, Director, Health Care Policy & Administration, CCHCS

Signature:_____ **Date:**_____
Gena Jones, **Director**, Division of Adult Institutions, CDCR

Signature:_____ **Date:**_____
Bryan Bishop, Director, Division of Adult Parole Operations, CDCR

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

DRAFT

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.

- **Medi-Cal PII** is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual. Medi-Cal 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, date and place of birth, mother's maiden name, driver's license number, or identification number. Medi-Cal PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. Medi-Cal PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

Appendix B - DHCS 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

DRAFT

- 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

DRAFT

Certification
- SIMM 5330-F – Information Security and Privacy Compliance and Enforcement Standard

DRAFT