



CITY OF WHEATLAND

CITY COUNCIL MEETING STAFF REPORT

June 13, 2023

SUBJECT: Council Approval of Yuba County's Response to Commercially Sexually Exploited Children/Youth Protocol Memorandum of Understanding

PREPARED BY: Damiean Sylvester, Police Chief

Recommendation

It is recommended that Council approve resolution 2023-XXXX to enter into the Yuba County's Response to Commercially Sexually Exploited Children/Youth Protocol (CSEC) Memorandum of Understanding (MOU) between the Health and Human Services Department, Child and Adult Protective Services Division, and the ten (10) participating agencies as referenced in the MOU.

Background

The Commercially Sexually Exploited Children/Youth (CSEC/Y) Program is administered by the California State Department of Social Services pursuant to SB 855. Commercially Sexually Exploited children/youth refers to those children and youth identified to be victims, or at risk of becoming victims, of commercial sexual exploitation (CSE). Yuba County has developed and will utilize a multidisciplinary team approach to CSEC/Y case management, service planning, and provision of services.

Pursuant to Welfare and Institutions Code 16524.8, Yuba County Health and Human Services Department has developed an interagency protocol MOU to be utilized in serving sexually exploited children. The MOU establishes guidelines for a multidisciplinary team approach to case management, service planning and provision of services for Commercially exploited children as required by the state.

The previous MOU has expired, and this is an update. The agreement has been reviewed and approved by city legal staff and no significant changes were made to the MOU.

Alternatives

None

Fiscal Impact

There is no financial impact to the General Fund.

Attachments

1. Resolution No. 18-23

RESOLUTION NO. 18-23

**RESOLUTION OF THE CITY COUNCIL OF THE CITY OF WHEATLAND FOR THE
WHEATLAND POLICE DEPARTMENT TO ENTER INTO A MEMORANDUM OF
UNDERSTANDING TO PARTICIPATE IN THE YUBA COUNTY COMMERCIALY
SEXUALLY EXPLOITED CHILDREN/YOUTH PROTOCOL**

WHEREAS a memorandum of understanding has been established between Yuba County and the City of Wheatland to participate in the Yuba County Commercially Sexually Exploited Children/Youth protocol.

NOW, THEREFORE, BE IT RESOLVED, by the City Council of the City of Wheatland as follows:

The City Council of the City of Wheatland authorizes the Police Chief, or designee to enter into the attached Memorandum of Understanding with Yuba County and partnering agencies.

I HEREBY CERTIFY that the foregoing resolution was duly and regularly introduced and adopted by the Council of the City of Wheatland, County of Yuba, State of California, held on the 13th day of June 2023 by the following vote:

AYES:

NOES:

ABSENT:

ABSTAIN:

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the official seal of said City this 13th day of June 2023.

ATTEST:

Lisa Thomason, City Clerk

Rick West, Mayor

The County of Yuba

HEALTH & HUMAN SERVICES DEPARTMENT

Jennifer Vasquez, Director

5730 Packard Ave., Suite 100, P.O. Box 2320, Marysville, California 95901
Phone: (530) 749-6311 FAX: (530) 749-6281



Phuong Luu, MD, MHS
Health Officer
Phone: (530) 749-6366

April 19, 2023

Damiean Sylvester
Chief of Police
Wheatland Police Department
207 Main Street
Wheatland, CA 95692

RE: CSEC Memorandum of Understanding (MOU)

Dear Chief Sylvester:

Enclosed, please find the Memorandum of Understanding (MOU) for the Yuba County Response to Commercially Sexually Exploited Children/Youth Protocol.

I would greatly appreciate it if you would obtain all signatures and dates where indicated for the City of Wheatland on **page 31**.

Please return the two (2) signed original signature pages to: Darcy Knox, Administrative Analyst, Yuba County Health and Human Services Department, 5730 Packard Ave. Suite 100, P.O. Box 2320, Marysville, CA 95901. I will route to other departments for signatures.

Upon receipt of the signed original MOUs I will submit them to the Yuba County Board of Supervisors for execution. I will return a copy of the fully executed MOU for your records.

Please feel free to contact Jessica Garcia, Program Manager, at (530) 749-6423 or by email at jgarcia@co.yuba.ca.us if there are any questions or concerns regarding this MOU.

Sincerely,

A handwritten signature in black ink, appearing to read "Darcy Knox", written in a cursive style.

Darcy Knox
Administrative Analyst

Enclosures

CITY OF WHEATLAND

By: _____
Rick West, Mayor

_____ Date

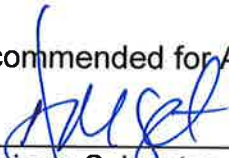
ATTEST:
City Clerk

By: _____
Lisa Thomason, City Clerk

APPROVED AS TO FORM:

By: _____
City Attorney

Recommended for Approval:



Damiean Sylvester, Chief of Police
Wheatland Police Department

6/6/2023
_____ Date

CITY OF WHEATLAND

By: _____
Rick West, Mayor

_____ Date

ATTEST:
City Clerk

By: _____
Lisa Thomason, City Clerk

APPROVED AS TO FORM:

By: _____
City Attorney

Recommended for Approval:



Damiean Sylvester, Chief of Police
Wheatland Police Department

6/6/2023
_____ Date

**YUBA COUNTY RESPONSE TO
COMMERCIALLY SEXUALLY EXPLOITED CHILDREN/YOUTH (CSE) PROTOCOL:
MEMORANDUM OF UNDERSTANDING**

I. OVERVIEW

The Commercially Sexually Exploited Children/Youth (CSEC/Y) Program is administered by the California State Department of Social Services (CDSS) pursuant to SB-855. Commercially Sexually Exploited Children/Youth refers to those minors under the age of 18, identified to be victims, or at risk of becoming victims, of commercial sexual exploitation (CSE). Yuba County has developed and will utilize a multidisciplinary team approach to CSEC/Y case management, service planning, and provision of services.

The following Community Partners to this Memorandum of Understanding (MOU) have agreed to participate in the Yuba County Commercially Sexually Exploited Children/Youth Protocol: Yuba County Health and Human Services Department, Child and Adult Protective Services (CAPS) Division, Sutter-Yuba Behavioral Health, Yuba County Juvenile Court, Yuba County Victim Services, Yuba County Counsel, Yuba County District Attorney's Office, Yuba County Public Defender, Yuba County Probation, and Law Enforcement Agency (i.e. Yuba County Sheriff's Department, Marysville Police Department, Wheatland Police Department, California Highway Patrol, and Yuba County Office of Education.

All participating community partners will assign personnel who have been trained to recognize the signs and symptoms of commercial sexual exploitation in order to engage any suspected CSE children and youth using best practice approaches.

1. Risk Factors

The following risk factors have been identified by Community Partners as being the most prevalent for children/youth in Yuba County:

- Child Welfare history
- Cutting/Self-Harm
- Developmental delays
- Drug or substance use
- Entertainment and modeling profession (interest or participation)
- Gang affiliation
- High number of moves in foster placement
- History of criminal record/arrest history/probation
- History of pregnancy or child birth
- History of sexual abuse
- Knows someone who has had sex in exchange for drugs, shelter, goods or money

- Lack of permanency – no adult or mentor they trust in their life
- Lesbian, Gay, Bi-Sexual, Transgender, Questioning, Queer, Intersex (LGBTQQI)
- Low school attendance/truancy/poor school performance
- Low self-esteem
- Migrant workers
- Multiple incidents of running away
- Probation
- Suicidal thoughts
- Tattoos/branding
- Signs that child/youth is underage
- Inconsistent personal information
- No identification
- Signs of physical and sexual violence
- Emotional distress
- Dominating or controlling relationship
- Inability to make eye contact
- Sexually provocative and/or weather inappropriate clothing
- Runaway/homeless/couch surfing
- Use of slang associated with sex industry

2. CSE and At-Risk Child/Youth Continuum of Care

The expectation is that Community Partners as a whole will collectively stress the importance of providing a continuum of care to CSEC/Y which will include: Trauma Informed Care, safety planning, and harm reduction.

Key Principles to serving CSEC/Y include:

- Safety planning for both the child/youth and the service providers
- Collaboration across agencies
- Trust and relationship building to foster consistency
- Culturally competent and appropriate service provision
- Trauma-informed intervention

II. FIRST RESPONDER PROTOCOL

The following community partners have been designated as those to be notified when a CSEC/Y has been identified:

- Appropriate Law Enforcement Agency for the active criminal investigation and coordination of evidence gathering;
- CAPS for the active abuse/neglect investigation, placement considerations and appropriate services;
- Yuba County Probation (if applicable) if the child victim becomes a Ward of the Court, and

- Yuba County Victim Services for victim advocacy, support, and services.

Yuba County Sheriff's Department, CAPS, Yuba County Probation and Yuba County Victim Services are Multi-Disciplinary Team (MDT) members and part of this protocol.

1. Law Enforcement Agency

1.1 Response

When responding to a call of alleged child/youth exploitation, the Law Enforcement Agency First Responder (hereinafter referred to as First Responder) will:

- 1.1.1** Identify the reporting party/witnesses and determine how the alleged crime(s) came to their attention.
- 1.1.2** Obtain a brief statement regarding the suspected exploitation. It is preferred that this information be gathered from a reliable adult, rather than the child/youth, whenever possible.
- 1.1.3** Identify the victim(s) and ensure their safety.
 - Obtain the child's/youth's name, date of birth, address, phone number, and relationship to the exploiter.
- 1.1.4** Coordinate with CAPS. All child sexual abuse reports must be cross-reported to CAPS at (530) 749-6288. If the exploiter is in the same home as the child/youth, or is the parent, CAPS must be contacted at the beginning of the incident response/investigation and a joint investigation is to be conducted at the response location.
- 1.1.5** Notify Yuba County Victim Services and request that an Advocate respond to the child's/youth's location (in accordance with California Penal Code §679.04). To request an Advocate, call Yuba County Victim Services at (530) 741-6275. After hours, First Responder will request Dispatch to notify the on-call Advocate.

1.2 Investigation/ Initial Interview

- 1.2.1** Record all interviews with all parties.
- 1.2.2** Gain minimal information from the victim and/or reporting party establishing that a crime has occurred. If the First

Responder must interview the victim to gain this information, do not get every date, incident, act, or details of the act. That information will be obtained during the Multidisciplinary Interview Center (MDIC) interview. Focus on when the last contact with the exploiter occurred, location of known incident(s), witnesses, and current location of the exploiter(s).

- **REMEMBER:** The First Responder may be able to get details from reliable parties other than the victim. Avoid interviewing the child/youth about this if this information is accessible from a reliable adult, parent, etc.
- **REMEMBER:** The First Responder should not interview the child/youth at the scene of the crime or near the exploiter. Avoid interviewing the child/youth in the presence of a parent, other adult, or another child/youth victim. If the child/youth must be interviewed, offer an Advocate in accordance with California Penal Code (PC) §679.04 and the CAPS worker (in a joint response call).

1.2.3 Obtain a recent photograph, if possible, of the alleged exploiter for identification purposes as well as any other potentially identifying information.

1.2.4 Identify other pertinent individuals who may have information regarding the allegations.

1.2.5 When possible, obtain detailed statements from these pertinent individuals regarding the incident(s) including age(s) of child/youth at the time of exploitation, date(s), time(s), and locations.

1.2.6 Gather relationship and contact information of all parties involved. If these individuals are not available, or if it is not possible to obtain their statements during the preliminary investigation, include information necessary to locate them.

1.2.7 Provide the non-offending care provider information about the MDIC interview and explain that someone will contact them to schedule a forensic interview with the victim.

1.3 Evidence Collection

1.3.1 Collect evidence at the crime scene, if indicated and available.

- The First Responder should consider obtaining search warrants as necessary to collect potentially valuable evidence (e.g., cell phones, cameras, computers, laptops, clothing, bedding, laundry, belts, weapons, other objects used to assault victim, lotion, lubricant, towels, and pornographic images and videos, etc.).
- Photograph the crime scene(s), if known, (e.g., bedrooms, bathrooms, etc.) depicting the layout of the home, park, school, etc.

1.3.2 Photograph the victim and any bruises, scratches, injuries, etc. (note that the Forensic Medical Examiner will do this as well.) Write the Police Report. If the responding officer talks to the child/youth, do not summarize what the child/youth said. Use direct quotes whenever possible. Avoid providing the child/youth with explanations and definitions that he/she does not use. It is imperative that the officer use the child's/youth's own words and not introduce words for genitalia. Avoid "yes" or "no" questions and remember to keep the discussion regarding the incident(s) brief. Write down what the child/youth says in an open narrative. Do not press the child/youth for details or clarification.

1.4 Multidisciplinary Interview (MDI) and Medical Exam Process

1.4.1 Initiate MDI process if there is an acute need for an MDI.

1.4.2 Authorize acute CSE medical exam.

- Law Enforcement Agency can authorize medical exams. All medical exams will need a Police Report Case Number assigned. To arrange a medical exam, the authorizing agency must fax the authorization form to the appropriate hospital staff personnel and agency.

1.4.3 During regular business hours, the investigating office shall contact a S.A.F.E clinic to arrange the medical exam. Victim Services may provide transportation to and from medical exams. After hours, the investigating office shall contact the S.A.F.E clinic to schedule a medical exam. The S.A.F.E examiner will inform the office of where the medical exam will take place. Medical exams will take place at the S.A.F.E clinic or in a hospital-based setting if needed. The Advocate can assist with these arrangements.

- Community Health providers may provide consultation on health issues pertaining to all children/youth identified as CSE or at high risk of CSE
- Notify CAPS or Yuba County Victim Services that CSE medical exam occurred.

1.4.4 Confer with Core CSEC/Y Team to determine best plan for child/youth.

2. CAPS

2.1 The intake worker (or on-call worker if after hours) will initiate a CSE Expedited Response by taking the following steps:

2.1.1 Obtain demographic information and allegation information.

2.1.2 Flag in CWS/CMS as “Commercially Sexually Exploited Child-CSEC” using Special Projects Code when triggering language (i.e. "CSEC in custody in the Pilot area") is used by the caller.

2.1.3 Initiate a CSE Referral.

2.1.4 Utilize Child Welfare Services/Case Management System (CWS/CMS) to determine if the child/youth has an open or prior case with CAPS.

2.1.5 Notify Yuba County Probation, Victim Services, and ongoing worker (if applicable), or assign new Social Worker to investigate.

2.1.6 CAPS will assign a Social Worker to attend the MDIC and briefing.

2.1.7 Determine the response and investigate if appropriate. Disposition may include one of the following responses: removal from parent or caregiver (utilize CSEC/Y approved placement when available), appropriate services as indicated by child/youth and family’s needs, or evaluate out.

2.1.8 Obtain a signed YCHHSD 452-1 Release of Information (Attachment A).

2.1.9 Utilize the WestCoast Children’s Clinic Commercial Sexual Exploitation – Identification Tool (CSE-IT) for screening. The

CSE-IT can be downloaded online at <http://www.westcoastcc.org/download-the-cse-it>.

2.1.10 If child/youth meets criteria for CAPS placement, within 72 hours CAPS will:

- Arrange for a full medical exam/Child Health and Disability Prevention (CHDP) assessment and mental health screening.
- Refer to contracted provider to initiate Child and Family Team (CFT) process.

2.1.11 If child/youth does not meet criteria for placement, CAPS will refer to contracted provider to initiate CFT process within ten (10) calendar days.

2.2 County Jurisdiction

2.2.1 When necessary, take the child/youth into protective custody pursuant to California Family Code §6250 or California Welfare and Institutions Code (WIC) §305.

2.2.2 Immediately after being transported to a place of safety, a child/youth ten (10) years of age or older shall be advised of their right to make at least two (2) telephone calls from the place where he or she is being held:

- A call to his/her parent, guardian, or responsible relative; and
- A call to a Public Defender [WIC § 308(b)].

2.2.3 If the child/youth identifies the exploiter, obtain Criminal Protective Order (CPO) and/or Temporary Protective Order (TRO) for no contact between victim and suspect.

2.2.4 When CSE victims are taken into protective custody by Law Enforcement Agency or CAPS, CAPS will determine the county of origin. If the county of origin is Yuba County, CAPS will assess the child/youth for placement needs and ongoing services.

2.2.5 If the child/youth has come from another county and that county has jurisdiction, then CAPS will communicate with the other county while transportation and placement arrangements are made. CAPS will attempt to have services

in place for the child/youth when they return to their county of residence.

2.3 Juvenile Court

The Juvenile Court of Yuba County will review all children/youth that committed an offense described in Section 602 of the Welfare and Institutions Code (WIC). In compliance with WIC 653.5, a probation officer shall immediately make any investigation he or she deems necessary to determine whether proceedings in the juvenile court shall be commenced. If it is believed the child/youth is a CSE victim, Yuba County Probation will work in collaboration with the CSEC/Y MDT to determine the most appropriate outcome for the child/youth.

2.4 Placement

CAPS and/or Yuba County Probation will establish safe and secure emergency transitional placements for CSE children/youth. Based on the situation, emergency placement may include the hospital, parents/guardians, an Intensive Therapeutic Foster Care (ITFC) home, or Short-Term Residential Therapeutic Program (STRTP). The CSEC/Y MDT is committed to providing the child/youth with services in their placement based on the child's/youth's needs.

3. Yuba County Victim Services

- 3.1** Arrange, coordinate and facilitate immediate crisis Core CSEC/Y Team (if applicable).
- 3.2** Arrange and coordinate Multidisciplinary Forensic Interview (MDFI) and request interviewer (if applicable).
- 3.3** Respond within 60 minutes.
- 3.4** Explain to child/youth the role of Yuba County Victim Services and engage with the child/youth to explain the process.
- 3.5** Provide access to a crisis counselor.
- 3.6** Provide assistance with the Criminal Protective Order and/or Temporary Restraining Order process.
- 3.7** Assist with arranging the CSE forensic medical exam.
- 3.8** Assist with arranging transportation to/from the CSE forensic medical exam.

- 3.9 Provide the child/youth with information and referrals specific to their needs.
- 3.10 Advocate for the child/youth.
- 3.11 Offer to contact the child/youth within three (3) working days after the initial contact. Follow up with the child/youth with their consent.

III. SCREENING, ASSESSMENT AND REFERRAL TO SERVICES

1. Identifying Commercial Sexually Exploited and At-Risk Children/Youth: WestCoast Children's Clinic Commercial Sexual Exploitation-Identification Tool (CSE-IT).

- 1.1 In order to understand the scope and nature of the problem in Yuba County and provide appropriate services, professionals will screen children/youth and assess their related needs on an ongoing basis utilizing the WestCoast Children's Clinic Commercial Sexual Exploitation-Identification Tool (CSE-IT).
- 1.2 The agency that completes the screening tool shall maintain the records of the screening results, including any information collected and statements made incident to the screening. This information will be shared with MDT agencies.
- 1.3 The screening tool's primary use is for the identification of CSE or at risk of becoming CSE. For any child/youth that is identified as CSE and/or in cases of imminent risk to a child/youth, call CAPS, 749-6288 and submit a Suspected Child Abuse Report (SCAR) to CAPS.
- 1.4 The screening tool will also be utilized to inform and improve service delivery. The agencies that complete the tool (not in the presence of the child/youth) will need to determine the level of risk the child/youth is at based on the number total from the questions that were answered by the screener. The screener at the agency will refer the child/youth to services in the community that will meet their needs or continue providing services for them.
- 1.5 The tool may to be used by professionals who work directly with children/youth. These professionals may include: CAPS, Yuba County Juvenile Probation, Yuba County Victim Services and Sutter-Yuba Behavioral Health partners.
- 1.6 All children/youth ages ten (10) and older will be screened regardless of gender. However, if children/youth under age ten (10) are suspected of being exploited, they will be screened.

- 1.7 The parties agree that the information and statements obtained from the child/youth as part of the screening process will be maintained, disclosed, and used only as follows and in accordance with all applicable state and federal laws and regulations. Information obtained from the screening shall be kept confidential and shall only be shared with other MDT agencies for purposes of identifying CSEC/Y.

2. Screening

The parties agree that a screen of an exploited child/youth's needs and strengths must take place upon identification and on an ongoing basis. Further, the parties agree that it is in the child's/youth's best interest to limit unnecessary and or duplicative screening. Accordingly, the parties will coordinate to ensure that screening are streamlined and limited when appropriate.

3. Referral to Behavioral Health Services

- 3.1 The parties will share information regarding the CSE-IT screening to limit the number of duplicative screening and potential for re-traumatization. The primary agency working with the child/youth will administer the CSE-IT Screening and obtain an Authorization to Release Information (Attachment B) so agencies can share information.
- 3.2 The person who administers the screening will communicate to child/youth, immediately prior to being screened, their personal rights as well as information sharing, confidentiality, and access to records.
- 3.3 The parties agree that the information and statements obtained from the child/youth as part of the screening process will be maintained, disclosed, and used in accordance with all applicable state and federal laws and regulations.
- 3.4 The person administering the screening shall make a child abuse and neglect report to CAPS, if the administrator has knowledge of or observes a child/youth in his or her professional capacity, or within the scope of his or her employment, whom he or she knows or reasonably suspects has been the victim of child abuse (PC 11166[a].)
- 3.5 The agency that completes the screening shall maintain the records of the screening, including any information collected and statements made incident to the screening.

- 3.6 Information obtained from the screening shall be kept confidential and shall only be shared with other MDT agencies for the purposes of identifying and providing services to support the CSEC/Y's treatment needs and assist in their recovery.

4. Victim Rights

4.1 Marsy's Law California Constitution, Article I, Section 28(b).

(b) In order to preserve and protect a victim's rights to justice and due process, a victim shall be entitled to the following rights:

- (1) To be treated with fairness and respect for his or her privacy and dignity, and to be free from intimidation, harassment, and abuse, throughout the criminal or juvenile justice process.
- (2) To be reasonably protected from the defendant and persons acting on behalf of the defendant.
- (3) To have the safety of the victim and the victim's family considered in fixing the amount of bail and release conditions for the defendant.
- (4) To prevent the disclosure of confidential information or records to the defendant, the defendant's attorney, or any other person acting on behalf of the defendant, which could be used to locate or harass the victim or the victim's family or which could disclose confidential communications made in the course of medical or counseling treatment, or which are otherwise privileged or confidential by law.
- (5) To refuse an interview, deposition, or discovery request by the defendant, the defendant's attorney, or any other person acting on behalf of the defendant, and to set reasonable conditions on the conduct of any such interview to which the victim consents.
- (6) To reasonable notice of and to reasonably confer with the prosecuting agency, upon request, regarding the arrest of the defendant if known by the prosecutor, the charges filed, the determination whether to extradite the defendant, and, upon request, to be notified of and informed before any pretrial disposition of the case.

- (7) To reasonable notice of all public proceedings, including delinquency proceedings, upon request, at which the defendant and the prosecutor are entitled to be present and of all parole or other post-conviction release proceedings, and to be present at all such proceedings.
- (8) To be heard, upon request, at any proceeding, including any delinquency proceeding, involving a post-arrest release decision, plea, sentencing, post-conviction release decision, or any proceeding in which a right of the victim is at issue.
- (9) To a speedy trial and a prompt and final conclusion of the case and any related post-judgment proceedings.
- (10) To provide information to the probation department official conducting a pre-sentence investigation concerning the impact of the offense on the victim and the victim's family and any sentencing recommendations before the sentencing of the defendant.
- (11) To receive, upon request, the pre-sentence report when available to the defendant, except for those portions made confidential by law.
- (12) To be informed, upon request, of the conviction, sentence, place and time of incarceration, or other disposition of the defendant, the scheduled release date of the defendant, and the release of or the escape by the defendant from custody.
- (13) To restitution:
 - (A) It is the unequivocal intention of the People of the State of California that all persons who suffer losses as a result of criminal activity shall have the right to seek and secure restitution from the persons convicted of the crimes causing the losses they suffer.
 - (B) Restitution shall be ordered from the convicted wrongdoer in every case, regardless of the sentence or disposition imposed, in which a crime victim suffers a loss.
 - (C) All monetary payments, monies, and property collected from any person who has been ordered to make restitution shall be first applied to pay the amounts ordered as restitution to the victim.

- (14) To the prompt return of property when no longer needed as evidence.
- (15) To be informed of all parole procedures, to participate in the parole process, to provide information to the parole authority to be considered before the parole of the offender, and to be notified, upon request, of the parole or other release of the offender.
- (16) To have the safety of the victim, the victim's family, and the general public considered before any parole or other post-judgment release decision is made.
- (17) To be informed of the rights enumerated in paragraphs (1) through (16).

A victim, the retained attorney of a victim, a lawful representative of the victim, or the prosecuting attorney upon request of the victim, may enforce the above rights in any trial or appellate court with jurisdiction over the case as a matter of right. The court shall act promptly on such a request. (Cal. Const., art. I, § 28(c) (1).)

4.2 Behavioral Health Client Rights

In accordance with Title 9, Chapter 4, Sections 10569 of the California Code of Regulations, each person receiving services shall have rights that include, but are not limited to, the following:

- (1) The right to confidentiality as provided for in Title 42, Code of Federal Regulations, Part 2.
- (2) To be accorded dignity in contact with agency staff.
- (3) To be accorded safe, healthful, and comfortable accommodations to meet his or her needs.
- (4) To be free from verbal, emotional, physical abuse and/or inappropriate sexual behavior.
- (5) To be informed by the program of the procedures to file a grievance or appeal discharge.
- (6) To be free from discrimination based on race, religion, sex, gender identity, ethnicity, age, disability, sexual orientation, and/or ability to pay.

(7) To be accorded access to his or her file.

IV. CSEC/Y MULTIDISCIPLINARY TEAM (MDT)

1. Formation of CSEC/Y Child Abuse Multidisciplinary Team (MDT)

1.1 WIC § 16524.6 specifically related to CSE describes MDT's serving this population to include, but not be limited to, staff from CAPS, Probation, Behavioral Health, substance abuse treatment providers, Community Health providers, local education agencies, local law enforcement, and survivors.

By this MOU, the parties are establishing a qualified child abuse multidisciplinary team ("MDT"), subject to the provisions contained in WIC § 18961.7. The parties agree that each of its staff participating in any convened MDT meeting are qualified under WIC § 18961.7 to participate in an MDT and have been trained in the prevention, identification, or treatment of child abuse and neglect.

The purpose of the MDT will be to allow all participating agencies to share confidential information in order to investigate reports of suspected child abuse and neglect and CSE referrals that are received. As part of the MDT, confidential information may be utilized to create a safety plan for the child/youth, identify the child's/youth's needs for proper placement and treatment, develop a plan to connect the child/youth to appropriate services and determine the appropriate placement for the child/youth. The following guidelines reflect statutory requirements under California law:

1.1.1 Given the complexities of the issues involved in CSE matters, the parties agree there is good cause to extend the 30-day period for members of the MDT to meet, disclose, and exchange information, documents, or any other material that relate to any incident of child abuse reported under this Protocol. This information may be exchanged, even though it also may be designated as confidential under state law, as long as a member of the MDT having the information reasonably believes it is generally relevant to the prevention, identification, or treatment of child abuse.

1.1.2 Any discussion relative to the disclosure or exchange of the information or writings during a team meeting is confidential and, notwithstanding any other law, testimony concerning that discussion is not admissible in any criminal, civil, or juvenile court proceeding.

- 1.1.3 Every MDT member who either receives information or records information regarding children and families in the capacity as an MDT member shall be under the same privacy and confidentiality obligations and subject to the same confidentiality penalties as the person disclosing or providing the information or records.
 - 1.1.4 All information or records obtained during the MDT meeting must be maintained in a manner that ensures the maximum protection of privacy and confidentiality rights. Disclosure and exchange of information shall not be made to anyone other than members of the MDT.
 - 1.1.5 Pursuant to WIC § 18964, an MDT may allow a parent, guardian, or other caregiver of the child/youth to attend the MDT meeting and provide information without becoming a member of the MDT. The individual must sign a written statement that he or she will not disclose any confidential information received as a result of attending the meeting.
 - 1.1.6 If a youth is a non-minor dependent, the MDT may have access to confidential records only with the explicit written and informed consent of the non-minor dependent.
- 1.2 The parties agree to provide staff to participate in MDT meetings who have been “trained in the prevention, identification or treatment of child abuse and neglect cases and who are qualified to provide a broad range of services related to child abuse and commercially sexually exploited children and those at risk for such exploitation.” In order to sufficiently address a commercially sexually exploited child/youth’s needs from identification through ongoing stabilization, a three-tiered multidisciplinary response, as described below, will be employed. This approach includes:
- 1.2.1 **Immediate Crisis MDT Meeting**, which involves both a rapid response within two (2) hours (this may be done by conference call) as well as intensive, ongoing support through the first 72 hours post-identification.
 - 1.2.2 **Initial MDT Meeting**, which includes convening a team within ten (10) days to address the child’s/youth’s needs after immediate safety risks have been addressed.
 - 1.2.3 **Ongoing MDT Meetings**, which include ongoing case planning and coordination. They may occur either on an individualized basis for each identified commercially sexually

exploited child/youth or in a broader case review setting, where multiple cases are reviewed on a regular basis during the monthly meeting.

1.3 The Steering Committee (refer to Section V. below for detailed information) is responsible for identifying required parties, as appropriate, to serve on the three (3) tiers of MDTs. Together the agencies represented on the Steering Committee will determine whether to include additional parties and to include in the MDTs in order to most effectively meet the unique needs of the child/youth. CAPS will be responsible for extending invitations to optional parties.

1.4 MDT meetings are collaborative and are not synonymous with the MDI process, which are conducted for investigative purposes.

2. Immediate Crisis Response MDT

The parties agree that children/youth who are suspected or identified victims of sexual exploitation and where an imminent risk to safety is present requires an immediate crisis response including initial engagement within two (2) hours (which may be via conference call), a child abuse investigation, and intensive services through the first 72 hours to stabilize them. See Immediate Crisis Response MDT section 2.10 for additional information.

The purpose of the Immediate Crisis Response CSEC/Y MDT is to provide a multidisciplinary team trained on CSE to each child/youth identified as exploited in order to immediately engage and stabilize the child/youth and develop a treatment plan that meets his/her needs in a coordinated manner. Designated team members will:

2.1 Respond to the child's/youth's location within two (2) hours.

2.2 Provide individual case-by-case collaboration with multiple child/youth-serving agencies.

2.3 Engage with the child/youth and family/caregiver(s), if appropriate.

2.4 Ensure basic needs are met such as food, shelter, and clothing.

2.5 Assess and address immediate and long-term needs.

2.6 Coordinate, monitor, and adjust the service plan to achieve desired outcomes for individual child/youth.

2.7 Advise on appropriate placement.

- 2.8** Conduct a safety plan upon placement with the parent/guardian/caregiver, which includes, but is not limited to the following:
 - 2.8.1** Ascertaining the potential safety risks for the child/youth, the family, and the providers.
 - 2.8.2** Identifying trauma triggers.
 - 2.8.3** Teaching techniques the child/youth can use to de-escalate when triggered.
 - 2.8.4** Deciding on steps team members will take to prevent a trigger from occurring.
 - 2.8.5** Delineating and documenting responsibilities of team members in the event a child/youth exhibits unsafe behavior. The team will involve the child/youth in planning and decision-making.

- 2.9** The following circumstances require an immediate response by the parties below:
 - 2.9.1** CAPS intake or on-call worker suspects or confirms that a child/youth is the victim of sexual exploitation or sex trafficking and there is an immediate safety concern;
 - 2.9.2** Law enforcement interacts with a child/youth they suspect or identify is a victim of commercial sexual exploitation and there is an immediate safety concern;
 - 2.9.3** Emergency response social worker assigned to a child abuse and neglect case suspects or confirms that a child/youth is the victim of sex trafficking and there is an immediate safety concern; and/or
 - 2.9.4** Medical professional treats a child/youth in the emergency room and suspects or confirms the child/youth is a victim of sex trafficking.

- 2.10** The following agencies are required to provide an immediate crisis response: Law Enforcement Agency, CAPS, Yuba County Probation, Yuba County District Attorney's Office and Yuba County Victim Services. In addition, the child/youth and the family may participate, if appropriate.

2.11 The responsibilities for each agency participating in the Immediate Crisis MDT are as follows:

2.11.1 CAPS

2.11.1.2 Intake Social Worker: Receive calls regarding suspected abuse and neglect, follow internal protocols, discern whether an allegation may involve commercial sexual exploitation, and if suspected or confirmed commercially sexually exploited child/youth:

- Determine the speed of the response, either Immediate Crisis or Initial MDT;
- Determine jurisdiction (either child welfare, probation, unknown);
- Based on determination of jurisdiction, contact Child Welfare Emergency Response or on-call worker for two (2) hour response; and
- Report to internal agency CSEC/Y Team Member who will report to Core CSEC/Y Team.

2.11.1.3 Emergency Response Social Worker: Respond to the child's/youth's location/staging area within two (2) hours when:

- The CSEC/Y is a dependent pursuant to WIC Section 300;
- The CSEC/Y is under Yuba County jurisdiction pursuant to WIC Section 241.1; and/or
- The CSEC/Y is not currently under the jurisdiction of any agency, but is alleged to be the victim of abuse, neglect, or exploitation.

2.11.2 Yuba County Probation Department

Respond within two (2) hours when: the CSEC/Y comes within the jurisdiction of the juvenile justice system pursuant

to WIC Section 602, et seq., or the CSE child/youth is within the jurisdiction pursuant to WIC § 241.1 and the Yuba County Probation Department is involved. Participate in the Immediate Crisis MDT when applicable.

2.11.3 Yuba County Victim Services

Serve as the lead agency, schedule and assemble the other team members when one (1) of the circumstances above occurs, and appoint someone to facilitate the Immediate Crisis MDT meeting. Provide individualized supports and services, including advocacy services to the child/youth. See initial response section 3.2 for additional details regarding the immediate crisis response from Yuba County Victim Services.

2.11.4 Law Enforcement

Participate in the Immediate Crisis MDT when applicable, to weigh in on the development of a treatment plan for immediate engagement and stabilization of the child/youth.

2.11.5 Yuba County District Attorney's Office

Participate in the Immediate Crisis MDT when applicable, to weigh in on the development of a treatment plan for immediate engagement and stabilization of the child/youth.

3. Initial Multidisciplinary Team

Not all children/youth that are suspected or identified victims of sexual exploitation or trafficking will be in imminent danger and require an Immediate Crisis response. An Initial MDT is an appropriate response when there is not an immediate safety risk but a child/youth is identified as or is suspected of being commercially sexually exploited.

For these non-urgent situations, the parties agree to coordinate and participate in an Initial MDT within ten (10) calendar days. This Initial MDT will assemble a team of individuals connected to the child's/youth's life to plan for the child's/youth's placement, safety, and well-being; provide individual case-by-case collaboration with multiple child/youth-serving agencies; ensure basic needs are met such as food, shelter, and clothing; assess and address immediate and long-term needs; coordinate the service plan; advise on appropriate placement; conduct safety plan once at the placement with parent/guardian/caregiver; ascertain the potential safety risks for the child/youth, the family, and the providers; identify trauma

triggers that may cause a child/youth to engage in unsafe behavior, coping skills the child/youth can use to de-escalate, and discuss steps team members will take to prevent a trigger from occurring; delineate and document responsibilities of team members in the event a child/youth exhibits unsafe behavior; and meaningfully involve child/youth in planning and decision-making.

The responsibilities of each party participating in the Initial MDT are as follows:

3.1 CAPS

3.1.1 Intake Social Worker: Receive calls regarding suspected abuse and neglect, follow internal protocols, discern whether an allegation may involve commercial sexual exploitation, and if suspected or confirmed commercially sexually exploited child/youth:

- Determine the speed of the response (either Immediate Crisis or Initial MDT);
- Determine jurisdiction (either child welfare, probation, or unknown);
- Based on determination of speed and jurisdiction, assign investigator to respond within ten (10) calendar days; and
- Report to internal agency CSEC/Y Team Member who will report to Core CSEC/Y Team.

3.1.2 Investigation Social Worker: Conduct child abuse investigation within ten (10) calendar days when the CSEC/Y is a dependent pursuant to WIC § 300.

3.2 Yuba County Victim Services

Serve as the lead agency, schedule and assemble the other team members when one (1) of the circumstances above occurs, appoint staff to facilitate the meeting, and discuss and refine the ongoing plan. Weigh in on an appropriate temporary placement, engage in safety planning, and identify and connect child/youth with community-based supports and services.

3.3 Sutter-Yuba Behavioral Health

Participate in the Initial MDT, if appropriate, to weigh in on an appropriate temporary placement, engage in safety planning, and identify and connect child/youth with community-based supports and services.

4. Ongoing Multidisciplinary Team (MDT)

4.1 Children/youth who are identified victims of sexual exploitation or trafficking require Ongoing MDT support to monitor the child/youth and ensure his/her needs are adequately addressed. These meetings shall be held monthly to monitor and support the child/youth and family (case planning, placement issues, safety planning etc.).

In addition to the statutorily required contact that parties have with children/youth under their jurisdiction, an Ongoing MDT meeting for an identified CSE should occur under the following circumstances including, but not limited to: once a month, when a child/youth runs away from placement/home/shelter, and when a child/youth prepares to testify in court case against exploiter/purchaser.

4.2 Long-term Support and Stabilization

The Ongoing MDT will continue to provide collaborative, long-term support to identified CSE including, but not limited to, referrals to services, connections with stable and supportive adults, and linkages to legal service providers to address civil legal issues.

V. STEERING COMMITTEE

As awareness of the problem of Commercial Sexual Exploitation of Children/Youth in the Yuba County region has grown, there has been a significant increase in the number of identified cases of CSE in the area. This has revealed challenges for responding effectively to these cases. To address the challenges identified the following actions and strategies shall be taken:

- The Steering Committee shall consist the following community agencies; Sutter-Yuba Behavioral Health, Yuba County Probation Department; Yuba County Health and Human Services; Yuba County District Attorney's Office; Yuba County Sherriff's Department; Yuba County Counsel; Marysville Police Department; Wheatland Police Department; and Yuba County Victim Services.
- Promote strategic collaboration and ongoing communication between all stakeholder agencies working directly with CSE cases;
- Identify and designate agency representative(s) who will serve as the liaison for communication with other partner agencies regarding CSE cases;

- Create reliable data documenting the results of service and system responses to CSE in the jurisdiction;
- For CSEC/Y who are in the juvenile justice system, establish quality programming and services that serve as alternatives to detention, detention stabilization, placement, and aftercare supports;
- Pursue sustainable funding to support the ongoing and effectiveness of the responses to this vulnerable population;
- Promote ongoing training for CSE knowledge and expertise.

In order to meet these needs, public and private agencies in the Yuba County area have actively partnered to increase communication, share decision making, and utilize necessary resources that result in improved safety and quality of life outcomes for identified CSEC/Y, while holding their traffickers criminally accountable for their actions.

1. Formation of a CSE Steering Committee

In order to best serve CSEC/Y in Yuba County, it is imperative that the agencies that interface with these children/youth do so collaboratively. Yuba County has formed its own countywide task force to more closely coordinate its efforts with respect to victims of child/youth commercial sexual exploitation. To ensure the effectiveness of the CSE Protocol, a County CSE Steering Committee has been formed. This committee will meet on an ongoing basis to review the protocol, identify what is working well, discuss any barriers that have arisen, and develop strategies to ensure the protocol runs efficiently.

1.1 Roles and Responsibilities

- 1.1.1 CAPS Facilitator:** Provides CSE Steering Committee coordination, administrative support and case management for dependency children/youth identified as CSE or at high risk of CSE.
- 1.1.2 Behavioral Health:** Provides, recommends, and coordinates behavioral health services to children/youth identified as CSE or at high risk of CSE.
- 1.1.3 Yuba County Counsel:** Ensures legal process and confidentiality for children/youth identified as CSE or at high risk of CSE.
- 1.1.4 Yuba County District Attorney:** Coordinates law enforcement investigation in cases involving all children/youth identified as CSE.

1.1.5 Law Enforcement Agency: Investigates cases involving children/youth suspected or identified as CSE.

1.1.6 Yuba County Probation: Provides case management for delinquency children/youth identified as CSE or at high risk of CSE.

1.1.7 Yuba County Victim Services: Provides MDT program coordination and facilitation, provides advocacy to children/youth and sexual abuse/trauma expertise to guide decisions regarding CSE policies and practices, provides, recommends and coordinates behavioral health services to children/youth identified as CSE or at high risk of CSE.

1.2 Practices

The CSE Steering Committee will designate a provider to conduct training for community stakeholders working with children/youth. The training will bring awareness to help identify sexually exploited and at-risk children/youth, provide services and support for CSE, as well as educate on the use of culturally competent and trauma-informed practices.

1.3 Prevention Efforts

Prevention efforts are designed to utilize outreach and education. Awareness training will be provided to foster and probation children/youth and students at local middle and high schools by the designated service provider. Prevention begins with identifying children/youth at risk for exploitation and connecting them with services and support before victimization occurs.

1.4 Target Population for Training Efforts

The CSE Steering Committee intends to make CSE training available to all Community Partners that directly work with children/youth. These agencies and individuals can assist with identifying and providing services to CSE and at-risk children/youth.

Identified target population includes, but is not limited to:

- California Youth Connection (CYC)
- Code Enforcement
- Community Schools
- Drug and Alcohol
- Independent Living Program (ILP)
- Juvenile Court
- Law Enforcement
- Behavioral Health

- Elementary Schools
- Emergency Medical Services/ Paramedics
- Faith based societies
- Family Resource Centers
- Fire Departments
- Foster parents
- Foster Parents Association
- Gay and Lesbian Alliances
- High Schools
- Homeless Shelters
- Middle Schools
- Nurses and Doctors
- Parents/Guardians
- Parks and Recreation
- Probation
- Sexual Assault Response Team (SART)
- Teachers
- Therapists
- Women's Shelter Program
- Yuba Community College

1.5 Data Collection

1.5.1 Protocols and strategies will be utilized to coordinate, collect, and share data across systems. This will be done to better understand the scope of work between agencies, identify issues within the system and process, track children/youth who have been sexually exploited, and document which resources are being used.

1.5.2 CAPS, Yuba County Probation and Yuba County Victim Services will be responsible for collecting and maintaining a data system that tracks the following: Number of children/youth screened, age, gender, risk level assessed, services provided, and name of agencies child/youth is referred to.

1.6 CSE Funding

Yuba County intends to utilize the funds pursuant to WIC § 16524.7(a)(4) as follows:

- Training for new staff and community partners
- Continuing education for existing staff
- Educating foster and probation youth
- Direct supports for CSE children/youth
- Resource Family supports
- CSEC/Y program supports
- Other Provider supports

VI. PRIVACY & SECURITY

1. CONFIDENTIALITY

- 1.1 All exchanged information by the parties and use and disclosure of such information under this MOU shall be in strict conformation with all applicable Federal, State and/or local laws and regulations relating to confidentiality including, but not limited to, the California Confidentiality of Medical Information Act (California Civil Code Section 56 *et seq.*), Welfare and Institutions Code Sections 5328 *et seq.*, 10850 and 14100.2, Health and Safety Code Sections 11977 and 11812.22, California Code of Regulations Section 51009, and 42 Code of Federal Regulations Section 2.1 *et seq.*, the California Department of Social Services (CDSS) Manual of Policies and Procedures, Division 19-0000, the California Department of Health Services Medi-Cal Eligibility Manual, Section 2H, the Medi-Cal Data Privacy and Security Agreement (Attachment C) between the California Department of Health Care Services and the County of Yuba and the Privacy and Security Agreement (Attachment D) between the California Department of Social Services and the County of Yuba to assure that all applications and records concerning program recipients shall be kept confidential and shall not be opened to examination, publicized, disclosed or used for any purpose not directly connected with administration of the program.
- 1.2 Each party shall inform all of its employees of the applicable confidentiality laws and regulations and that any person knowingly and intentionally violating such laws and regulations may be guilty of a misdemeanor.
- 1.3 Each party is responsible for monitoring its compliance with all State and Federal statutes and regulations regarding confidentiality. Each party shall ensure that no list of persons receiving services under this MOU is published, disclosed, or used for any other purpose except for the direct administration of the program/services or other uses authorized by law that are not in conflict with requirements of confidentiality.
- 1.4 Except as otherwise provided in this MOU, each party may use or disclose protected health information (PHI) and/or personally identifiable information (PII) to perform functions, activities or services for or on behalf of each party, as specified in this MOU, provided that such use or disclosure shall not violate the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("HITECH Act") and associated regulations at 45 CFR Parts 160, 162, and 164. The uses and disclosures of PHI may not be more expansive than those applicable to each party, as the "Covered Entity" under the Privacy Rule, except

as authorized for management, administrative or legal responsibilities of each party.

- 1.5 None of the parties shall use or further disclose PHI and/or PII other than as permitted or required by this MOU, or as required by law.
- 1.6 Each party shall implement administrative, physical and technical safeguards that are reasonable and appropriately protect the confidentiality, integrity and availability of PHI/PII that is disclosed or received by the other party.
- 1.7 Each party shall ensure that any agent, including a subcontractor to whom each party provides PHI/PII, or to whom each party provides PHI/PII which is disclosed or received by the other parties, is allowable by law and that the agent/subcontractor agrees to the same restrictions and conditions that apply to each party with respect to such information.
- 1.8 Each party shall make internal records related to the use, disclosure, and privacy protection of PHI received from each other available to each other or to the Secretary of the United States Department of Health and Human Services for purposes of investigating or auditing compliance with HIPAA or other laws or regulations, in a time and manner designated by each party.
- 1.9 The parties agree to take such action as is necessary to amend this MOU as necessary for each party to comply with Federal, State and/or local laws and regulations relating to confidentiality and privacy and security rules.
- 1.10 Each party shall mitigate, to the extent practicable, any harmful effect that is known to each other of a use or disclosure of PHI/PII by each party in violation of the requirements of this MOU or Federal, State, or local confidentiality laws or regulations.

2. DATA SECURITY

- 2.1 Confidential information transmitted by the parties by means of electronic transmissions must be encrypted according to Advanced Encryption Standards (AES) of 128 BIT or higher. Additionally, a password or pass phrase must be utilized.
- 2.2 Each party shall inform the other in writing within five (5) working days of any security incident of which each party becomes aware. It is understood that if the security breach incident is not corrected within sixty (60) days of the written notification, each party acknowledges that any party may terminate this MOU.

2.3 Each party is responsible to immediately notify each other of any breaches or potential breaches of security related to each party's confidential information, data maintained in computer files, program documentation, data processing systems, data files and data processing equipment which stores or processes each other's data internally or externally.

2.4 In the event of a breach of security related to confidential client information provided to each other, each party will manage the response to the incident, however, each party may be responsible to issue any notification to affected individuals as required by law or as deemed necessary by each party's discretion. Each party will be responsible for all costs incurred as a result of providing the required notification.

VII. TERMINATION

Notwithstanding any other provision of this MOU, this MOU may be terminated by any of the parties without cause upon thirty (30) days written notice to the other parties.

VIII. NOTICES

Any notice required or permitted to be given under this MOU shall be in writing and shall be served by mail. Notices shall be addressed as follows:

If to YUBA COUNTY HEALTH AND HUMAN SERVICES DEPARTMENT: Jennifer Vasquez, Director Yuba County Health and Human Services Department 5730 Packard Ave., Ste 100 P.O. Box 2320 Marysville, CA 95901	With a copy to: County Counsel County of Yuba 915 8th St., Suite 111 Marysville, CA 95901
---	---

If to YUBA COUNTY DISTRICT ATTORNEY'S OFFICE Clint Curry, District Attorney Yuba County District Attorney's Office 215 5 th Street Marysville, CA 95901	With a copy to: County Counsel County of Yuba 915 8th St., Suite 111 Marysville, CA 95901
--	---

If to YUBA COUNTY SHERIFF'S DEPARTMENT Wendell Anderson, Sheriff Yuba County Sheriff's Department 720 Yuba Street Marysville, CA 95901	With a copy to: County Counsel County of Yuba 915 8th St., Suite 111 Marysville, CA 95901
--	---

If to YUBA COUNTY PROBATION DEPARTMENT

Jim Arnold, Chief Probation Officer
Yuba County Probation Department
215 5th Street
Marysville, CA 95901

With a copy to:

County Counsel
County of Yuba
915 8th St., Suite 111
Marysville, CA 95901

If to MARYSVILLE POLICE DEPARTMENT

Chris Sachs, Chief of Police
Marysville Police Department
316 6th Street
Marysville, CA 95901

With a copy to:

If to WHEATLAND POLICE DEPARTMENT

Damiean Sylvester, Chief of Police
Wheatland Police Department
207 Main Street
Wheatland, CA 95692

With a copy to:

If to SUTTER-YUBA BEHAVIORAL HEALTH:

Rick Bingham
Director for Behavioral Health
Sutter-Yuba Behavioral Health
1965 Live Oak Blvd, Suite A
P.O. Box 1520
Yuba City, CA 95992-1520

With a copy to:

County Counsel
County of Sutter
1160 Civic Center Drive, Suite C
Yuba City, CA 95993

IN WITNESS WHEREOF, this MOU has been executed as follows:

YUBA COUNTY BOARD OF SUPERVISORS

By: _____
Andy Vasquez Jr., Chair

Date: _____

ATTEST: MARY PASILLAS
YUBA COUNTY CLERK OF THE BOARD

APPROVED AS TO FORM:
YUBA COUNTY COUNSEL

Michael J. Ciccozzi

Recommended for Approval:

Clint Curry, District Attorney
Yuba County District Attorney's Office

Date

Wendell Anderson, Sheriff
Yuba County Sheriff's Department

Date

Jim Arnold, Chief Probation Officer
Yuba County Probation Department

Date

Jennifer Vasquez, Director
Yuba County Health and Human Services Department

Date

CITY OF MARYSVILLE

By: _____
Chris Branscum, Mayor

_____ Date

ATTEST:
City Clerk

By: _____
Nicole Moe, City Clerk

APPROVED AS TO FORM:

By: _____
City Attorney

Recommended for Approval:

Chris Sachs, Chief of Police
Marysville Police Department

_____ Date

CITY OF WHEATLAND

By: _____
Rick West, Mayor

Date

ATTEST:
City Clerk


By: _____
Lisa Thomason, City Clerk

APPROVED AS TO FORM:

By:  _____
Cindy J. Bann
City Attorney

Recommended for Approval:


Damiean Sylvester, Chief of Police
Wheatland Police Department



Date

SUTTER-YUBA BEHAVIORAL HEALTH

SUTTER COUNTY BOARD OF SUPERVISORS

By: _____
Chair

Date: _____

ATTEST: DONNA M. JOHNSTON
SUTTER COUNTY CLERK OF THE BOARD

APPROVED AS TO FORM:
SUTTER COUNTY COUNSEL

Recommend for Approval:

Director
Sutter-Yuba Behavioral Health

Date

ATTACHMENT A



AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION, PERSONALLY IDENTIFIABLE INFORMATION, AND/OR OTHER CLIENT/PATIENT CASE RELATED INFORMATION

Facility/Provider Information

Name of Facility/Provider: _____
Street Address: _____
City: _____ State: _____ Zip: _____
Phone Number: (_____) _____ Fax Number: (_____) _____

Client/Patient Information

Name of Client/Patient: _____
Street Address: _____
City: _____ State: _____ Zip: _____
Phone Number: (_____) _____ Date of Birth: _____
Other Identifying Name (AKA): _____

I authorize the facility/provider listed above to release medical services, social services, drug, and alcohol services, and/or mental health services information about me (AS DESCRIBED BELOW).

Release Information to:

Name of Agency/Person: _____
Street Address: _____
City: _____ State: _____ Zip: _____
Phone Number: (_____) _____ Fax Number: (_____) _____

The information to be disclosed includes (indicate choice by initialing specific items):

- All medical information.
- Only the following information (specify information below, e.g., "discharge summary only"):

I specifically authorize the release of the following information:

- HIV/AIDS
- Behavioral Health
- Psychological Testing Results
- Drug/Alcohol Treatment

This disclosure of information is for the following purpose:

- At the request of the individual.
- Other (describe specific purpose): _____

If not revoked, this authorization shall terminate after one (1) year:

- Other date: _____ (must be less than one (1) year)

I understand the following about this authorization:

- I can revoke this authorization in writing. Requests to revoke authorizations must be made in writing to our department. For additional information see our Notice of Privacy Practices.
- I understand treatment cannot be denied to me based on my refusal to sign this authorization. However, outside agencies which require protected health information to provide various services to or for me may not be able to do so without this information.
- If the organization I have authorized to receive information is not a health plan or health care provider, the released information may no longer be protected by federal privacy regulations
- Disclosures resulting from this authorization may be in written, electronic, and/or verbal form.
- I have a right to receive and I will be offered a copy of this authorization.
- A copy of this authorization is as valid as an original.

Signature of: _____ Date: _____

- Client/Patient
- Patient Representative (Indicate relationship, e.g., parent, guardian, conservator):

Witness: _____ Date: _____

County Staff Use Only		
Initials of Staff Receiving Form	Mailed/Faxed By	Date Mailed/Faxed
Additional Notes: 		



**Departamento de Salud y Servicios Humanos del Condado de Yuba
Autorización para Revelar Información Protegida Acerca de Salud,
Información de Identificación Personal, y/o Cualquier Información
Relacionada al Cliente/Paciente**

Establecimiento/Proveedor

Nombre del Establecimiento/Proveedor: _____

Dirección del Establecimiento/Proveedor: _____

Ciudad: _____ Estado: _____ Código Postal: _____

Numero de Teléfono: (_____) _____ Numero de Fax: (_____) _____

Información del Cliente/Paciente

Nombre Completo del Cliente/Paciente: _____

Dirección del Cliente/Paciente: _____

Ciudad: _____ Estado: _____ Código Postal: _____

Numero de Teléfono #: (_____) _____ Fecha de Nacimiento: _____

Otro Nombre de Identificación (ALIAS): _____

Yo autorizo al establecimiento/proveedor medico anotado arriba a compartir información sobre servicios médicos, servicios sociales, servicios de drogas y alcohol, y/o servicios de salud mental sobre mí (COMO SE DESCRIBE ABAJO).

Compartir Información a:

Nombre de la Agencia / Persona : _____

Dirección de la Agencia / Persona: _____

Ciudad: _____ Estado: _____ Código Postal: _____

Numero de Teléfono #: (_____) _____ Numero de Fax: (_____) _____

La información que se revelará incluye (indique su elección con sus iniciales en artículos específicos):

Toda la información médica.

Únicamente la siguiente información (especifique, por ejemplo "resumen de alta médica"):

Autorizo específicamente la revelación de la siguiente información:

- VIH/Sida
- Salud Mental
- Resultados de las Pruebas Psicológicas
- Tratamiento de Drogas/Alcohol

Esta revelación de información es para la siguiente razón:

- A petición de la persona.
- Otro (describa el propósito específico): _____

Si esta autorización no es revocada, se dará por terminado después de un (1) año:

- Otro fecha: _____ (debe ser menos de un (1) año)

Entiendo lo siguiente acerca de esta autorización:

- Yo puedo revocar esta autorización por escrito. La solicitud de revocación de autorizaciones debe ser por escrito a nuestro departamento. Para obtener información adicional consulte a nuestro Aviso Sobre Practicas de Privacidad.
- Yo entiendo que tratamiento para mí no puede ser negado por mi rechazo de firmar esta autorización. Sin embargo, agencias externas que requieren información protegida para proveerme varios servicios, no podrán ser capaz de hacerlo sin esta información.
- Si la organización que he autorizado a recibir información no es de un plan de salud o proveedor de salud, puede que la información revelada ya no esté protegida por las regulaciones federales de privacidad.
- Revelaciones resultando de esta autorización pueden ser en forma escrita, electrónicamente, y/o verbalmente.
- Tengo derecho a recibir y se me ofrecerá una copia de esta autorización.
- Una copia de esta autorización es tan válida como la original.

Firma de: _____ Fecha: _____

- Cliente/Paciente
- Representante del Paciente (Indica la relación. Por ejemplo, los padres, guardián, conservador):

Testigo: _____ Fecha: _____

County Staff Use Only		
Initials of Staff Receiving Form	Mailed/Faxed By	Date Mailed/Faxed
Additional Notes: 		



**DAIM NTAUV TSOCAI TSO TAWM NTAWM COV NTAUB NTAUV
KHOMOB RAUG TXWV, NTAUB NTAUV QHIA HAIS TXOG TUS
KHEEJ, THIAB/LOSSIS LWM YAM NTAUB NTAUV TXOG NTAWM TUS
NEEG/TUS NEEG MOB**

Chaw Kuaj/Kws Khomob

Chaw Kuaj/Kws Khomob: _____

Chaw Kuaj/Kws Khomob Chaw Nyob: _____

Zos: _____ Xeev: _____ Ziv Khauj: _____

Xovtooj: (_____) Xovtooj Xa Ntawv: (_____)

Tus Neeg Mob Lub Npe

Tus Neeg Mob Lub Npe: _____

Tus Neeg Mob Qhov Chaw Nyob: _____

Zos: _____ Xeev: _____ Ziv Khauj: _____

Xovtooj: (_____) Hnub Yug: _____

Siv dua lwm lub npe (Hu Tias): _____

Kuv tsocai rau qhov chaw/kws khomob muaj npe saum no tso tawm cov ntaub ntawv khomob, kev pabcuam, pabcuam tshuj thiab cawv thiab/lossis khomob puas hlwb hais txog kuv (LI PIAV NRAM NO).

Tso Cov Ntawv Kho Mob Rau:

Lub Koom Haum/Tus Neeg Tso Cai Rau: _____

Chaw Nyob: _____

Zos: _____ Xeev: _____ Ziv Khauj: _____

Xovtooj: (_____) Xovtooj Xa Ntawv: (_____)

Cov ntaub ntawv qhib tso tawm (sau thawj ob tug niam ntawv ntawm lub npe ua koj qhov kev xaiv):

_____ Txhua yam ntaub ntawv kho mob nkeeg.

_____ Tsuas yog cov ntaub ntawv kho mob qhia nram no xwb (pivtxwv, "ntaub ntawv tso tawm mus tsev"):

_____ Kuv hais qhia meej kom tso tawm cov kev kho mob teev nram no:

- Kho mob HIV/AIDS
- Kho mob puas hlwb
- Kev qhia ntawm qhov kev kuaj seb puas yog neeg puas hlwb
- Kev kho mob txog kev quav yeeb quav tshuj/cawv

Qhov kev thov qhib ntawm cov ntaub ntawv yog muaj raws li qhov tseem ntsiab nram no:

Yog kev thov los ntawm tus kheej.

Lwm yam (qhia kom meej seb yog dabtsi): _____

Yog tias tsis thim, daim ntawv tsocai no yuav siv tsis tau ntxiv tomaqab (1) xyoos:

Lwm lubcaij _____ (Yuav tsum yog tsawg tshaj ib (1) xyoos)

Kuv nkag siab cov nram qab no hais txog daim ntawv tsocai:

- Kuv muaj cuabkav thim daim ntawv no sau ua ntaub ntawv. Thov thim yuav tsum yog sau ua ntaub ntawv rau peb cov ua haujlwm. Xav paub ntxiv, saib rau peb Kev Ceebtoom Txog Kev Ceev Ntaub Ntawv.
- Kuv nkag siab tias kev kho yuav tsis raug txiav yog tias kuv tsis kam suam npe rau daim ntawv tsocai no. Txawm licias los xij, lwm lub koomhaum sab nraud uas xav tau cov ntaub ntawv kho mob rau cov kev pabcuam rau kuv yuav tsis tau txais yog kuv tsis kam suam npe rau daim ntawv tsocai no.
- Yog tias lub koomhaum uas kuv tsocai tau txais cov ntaub ntawv kho mob no tsis yog txoj kev npaj kho mob lossis tsis yog chaw kho mob, cov ntaub ntawv tso tawm no yuav tsis raug fivthaiv lawm raws li tsoom fww qibsiab cov kev cai ceev ntaub ntawv.
- Kev qhib ntawm daim ntawv tsocai no yog sau ua ntaub ntawv, tawm faifab, thiab/lossis ua lus tham.
- Kuv muaj cai tau txais thiab kom luam ib tsab ntawm daim ntawv tsocai no rau kuv.
- Luam ib tsab ntawm daim ntawv tsocai no siv tau ib yam li yog daim tseem.

Tus Suam Npe: _____ Hnub Tim: _____

Tus Neeg Mob

Sawvcev Tus Neeg Mob - Yog tias tus sawvcev suam npe, qhia seb txheeb licias (niam/txiv, tus saib, tus muaj cai saib xyuas):

Povthawj: _____ Hnub Tim: _____

County Staff Use Only		
Initials of Staff Receiving Form	Mailed/Faxed By	Date Mailed/Faxed
Additional Notes:		

ATTACHMENT B

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

PLEASE PRINT OR TYPE **INSTRUCTIONS AVAILABLE ON REQUEST**

Obtain From Facility/Provider:		Patient's Full Name:	Phone #
Address:		Address:	
		Date of Birth:	
Phone #	Fax #	Other Identifying Name	Clinic Number

I authorize the facility/provider listed above to release medical information about me to the following (if I am authorizing the release of substance use disorder information to a non-treating individual, I must specify the name of each individual recipient):

Please release information to:	Additional Information: Phone #: _____ Fax #: _____
Please release information to:	Additional Information: Phone #: _____ Fax #: _____
Please release information to:	Additional Information: Phone #: _____ Fax #: _____
Please release information to:	Additional Information: Phone #: _____ Fax #: _____
Please release information to:	Additional Information: Phone #: _____ Fax #: _____

The information to be disclosed shall be limited to the following (indicate choices by initialing the blanks):

- My complete medical record **excluding** information related to use of psychiatric conditions, HIV/AIDS or substance use disorders (unless initialed below).
- Psychiatric HIV/AIDS

(continued on next page)

SUTTER-YUBA BEHAVIORAL HEALTH SERVICES

V. 6/2/2020

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

- Substance Use Disorder Services (to include):
- Assessment, diagnosis, Treatment & Discharge plan and/or prognosis
 - Substance use history
 - Progress notes and details of client participation
 - Periodic reports on progress in treatment and prognosis
 - Results of drug testing
 - Billing records

Other (be specific): _____

This disclosure of information is for the following purpose:

- At the request of the individual (no further explanation of purpose required)
 Evaluation Case Planning Other: _____

If not revoked, this authorization shall terminate after (check one):

- 6 months 1 year Other date: _____

I understand the following about this authorization:

- I can revoke this authorization in writing. Requests to revoke authorizations must be made in writing at the Medical Records Office where this form originated. For additional information see our Notice of Privacy Practices.
- We will not deny treatment to you based on your refusal to sign this authorization. However, outside agencies which require protected health information to provide various services to, or for you, may not be able to provide those services.
- If the organization I have authorized to receive the information is not a health plan or health care provider, the released information may no longer be protected by federal privacy regulations.
- Disclosures resulting from this authorization may be in written, electronic, and/or verbal form.
- I have a right to receive and I will be offered a copy of this authorization.
- A copy of this authorization is as valid as an original.

Date: _____

Signature of Client/Patient Patient Representative (e.g., parent, guardian, conservator)

If patient representative, enter relationship: _____

Witnesses: If signed with a mark, two witnesses' signatures are required at right. One witness must also print the patient's or patient rep's name by the mark.

	Witness	Date
	Witness	Date

COUNTY STAFF USE ONLY

Initials of staff receiving form:	Mailed by:	Date Mailed:
-----------------------------------	------------	--------------

SUTTER-YUBA BEHAVIORAL HEALTH SERVICES

V. 6/2/2020

ATTACHMENT C

515-2019

MEDI-CAL PRIVACY & SECURITY AGREEMENT NO.: 19 - 58

MEDI-CAL PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Health Care Services and the
County of Yuba,
Department/Agency of Health and Human Services.

PREAMBLE

The Department of Health Care Services (DHCS) and the
County of Yuba
Department/Agency of Health and Human Services
(County Department) enter into this Medi-Cal Privacy and Security Agreement
(Agreement) in order to ensure the privacy and security of Medi-Cal Personally
Identifiable Information (Medi-Cal PII).

DHCS receives federal funding to administer California's Medicaid Program
(Medi-Cal). The County Department/Agency assists in the administration of Medi-Cal, in
that DHCS and the County Department/Agency access DHCS eligibility information for
the purpose of determining Medi-Cal eligibility.

This Agreement covers the
County of Yuba
Department/Agency of Health and Human Services
workers, who assist in the administration of Medi-Cal; and access, use, or disclose
Medi-Cal PII.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. **"Assist in the administration of the Medi-Cal program"** means performing administrative functions on behalf of Medi-Cal, such as establishing eligibility, determining the amount of medical assistance, and collecting Medi-Cal PII for such purposes, to the extent such activities are authorized by law.
2. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized

purposes have access or potential access to Medi-Cal PII, whether electronic, paper, verbal, or recorded.

3. **"County Worker"** means those county employees, contractors, subcontractors, vendors and agents performing any functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII.
4. **"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 (SSN), date and place of birth (DOB), 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.
5. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Medi-Cal PII, or interference with system operations in an information system which processes Medi-Cal PII that is under the control of the County or County's Statewide Automated Welfare System (SAWS) Consortium, or a contractor, subcontractor or vendor of the County.
6. **"Secure Areas"** means any area where:
 - A. County Workers assist in the administration of Medi-Cal;
 - B. County Workers use or disclose Medi-Cal PII; or
 - C. Medi-Cal PII is stored in paper or electronic format.
7. **"SSA-provided or verified data (SSA data)"** means:
 - A. Any information under the control of the Social Security Administration (SSA) provided to DHCS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or
 - B. Any information provided to DHCS, including a source other than SSA, but in which DHCS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State

and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

AGREEMENTS

DHCS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

- A. County Department/Agency County Workers may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal in accordance with Section 14100.2 of the Welfare and Institutions Code, Section 431.300 et. Seq. of Title 42 Code of Federal Regulations, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of a Medi-Cal client are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.
- B. Pursuant to this Agreement, County Workers may only use Medi-Cal PII to assist in the administration of the Medi-Cal program.
- C. Access to Medi-Cal PII shall be restricted to County Workers who need to perform their official duties to assist in the administration of Medi-Cal.
- D. County Workers who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

The County Department/Agency agrees to advise County Workers who have access to Medi-Cal PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department/Agency shall implement the following personnel controls:

- A. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:
 - 1. Provide initial privacy and security awareness training to each new County Worker within 30 days of employment;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three or more security reminders per year are recommended;
3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed and;
4. Retain training records for a period of three years after completion of the training.

B. *Employee Discipline.*

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

- C. *Confidentiality Statement.*** Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three years, or five years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

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

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

D. *Background Screening.*

1. Conduct a background screening of a County Worker before they may access Medi-Cal PII.
2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3. The County Department/Agency shall retain each County Worker's background screening documentation for a period of three years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

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

- A. Conduct periodic privacy and security review of work activity by County Workers, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of Medi-Cal PII.
- B. The periodic privacy and security reviews shall be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of the Medi-Cal program, and the use or disclosure of Medi-Cal PII.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department/Agency agrees to:

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

V. PHYSICAL SECURITY

The County Department/Agency shall ensure Medi-Cal PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The County Department/Agency agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

- A. Secure all areas of the County Department/Agency facilities where County Workers assist in the administration of Medi-Cal and use, disclose, or store Medi-Cal PII.

- B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
 - 1. Properly coded key cards
 - 2. Authorized door keys
 - 3. Official identification
- C. Issue identification badges to County Workers.
- D. Require County Workers to wear these badges where Medi-Cal PII is used, disclosed, or stored.
- E. Ensure each physical location, where Medi-Cal PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.
- F. Ensure there are security guards or a monitored alarm system at all times at the County Department/Agency facilities and leased facilities where 500 or more individually identifiable records of Medi-Cal PII is used, disclosed, or stored. Video surveillance systems are recommended.
- G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of Medi-Cal PII have perimeter security and physical access controls that limit access to only authorized County Workers. Visitors to the data center area shall be escorted at all times by authorized County Workers.
- H. Store paper records with Medi-Cal PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County Department/Agency and non-County Department/Agency functions in one building in work areas that are not securely segregated from each other. It is recommended that all Medi-Cal PII be locked up when unattended at any time, not just within multi-use facilities.
- I. The County Department/Agency shall have policies based on applicable factors that include, at a minimum, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles shall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit Medi-Cal PII be left unattended in a vehicle overnight or for other extended periods of time.

- J. The County Department/Agency shall have policies that indicate County Workers are not to leave records with Medi-Cal PII unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

VI. **TECHNICAL SECURITY CONTROLS**

- A. ***Workstation/Laptop Encryption.*** All workstations and laptops, which use, store and/or process Medi-Cal PII, shall be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- B. ***Server Security.*** Servers containing unencrypted Medi-Cal PII shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- C. ***Minimum Necessary.*** Only the minimum necessary amount of Medi-Cal PII required to perform required business functions may be accessed, copied, downloaded, or exported.
- D. ***Mobile Device and Removable Media.*** All electronic files, which contain Medi-Cal PII, shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption shall be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- E. ***Antivirus Software.*** All workstations, laptops and other systems, which process and/or store Medi-Cal PII, shall install and actively use an anti-virus software solution. Anti-virus software should have automatic updates for definitions scheduled at least daily.
- F. ***Patch Management.***
 - 1. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, shall have critical security patches applied, with system reboot if necessary.

SSA data via Medi-Cal Eligibility Data System (MEDS), and over the process of issuing and maintaining access control numbers, IDs, and passwords.

- I. **Data Destruction.** When no longer needed, all Medi-Cal PII shall be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Medi-Cal PII cannot be retrieved.
- J. **System Timeout.** The systems providing access to Medi-Cal PII shall provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- K. **Warning Banners.** The systems providing access to Medi-Cal PII shall display a warning banner stating, at a minimum:
 - 1. Data is confidential;
 - 2. Systems are logged;
 - 3. System use is for business purposes only, by authorized users; and
 - 4. Users shall log off the system immediately if they do not agree with these requirements.
- L. **System Logging.**
 - 1. The systems that provide access to Medi-Cal PII shall maintain an automated audit trail that can identify the user or system process which initiates a request for Medi-Cal PII, or alters Medi-Cal PII.
 - 2. The audit trail shall:
 - a. Be date and time stamped;
 - b. Log both successful and failed accesses;
 - c. Be read-access only; and
 - d. Be restricted to authorized users of the audit trail.
 - 3. If Medi-Cal PII is stored in a database, database logging functionality shall be enabled.
 - 4. Audit trail data shall be archived for at least three years from the occurrence.
- M. **Access Controls.** The system providing access to Medi-Cal PII shall use role based access controls for all user authentications, enforcing the principle of least privilege.

N. *Transmission Encryption.*

1. All data transmissions of Medi-Cal PII outside of a secure internal network shall be encrypted using a FIPS 140-2 certified algorithm that is 128 bit or higher, such as AES or TLS. It is encouraged, when available and when feasible, that 256 bit encryption be used.
2. Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted.
3. This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and email.

- O. ***Intrusion Prevention.*** All systems involved in accessing, storing, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, shall be protected by an intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. *System Security Review.*

1. The County Department/Agency shall ensure audit control mechanisms are in place.
2. All systems processing and/or storing Medi-Cal PII shall have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
3. Reviews should include vulnerability scanning tools.

- B. ***Log Reviews.*** All systems processing and/or storing Medi-Cal PII shall have a process or automated procedure in place to review system logs for unauthorized access.

- C. ***Change Control.*** All systems processing and/or storing Medi-Cal PII shall have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

- D. ***Anomalies.*** When the County Department/Agency or DHCS suspects MEDS usage anomalies, the County Department/Agency shall work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to DHCS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

- A. **Emergency Mode Operation Plan.** The County Department/Agency shall establish a documented plan to enable continuation of critical business processes and protection of the security of Medi-Cal PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours. It is recommended that counties conduct periodic disaster recovery testing, including connectivity exercises conducted with DHCS, if requested.
- B. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of Medi-Cal PII, shall include environmental protection such as cooling; power; and fire prevention, detection, and suppression; and appropriate protection from other threats, including but not limited to flood, earthquake, and terrorism.
- C. **Data Backup Plan.**
 - 1. The County Department/Agency shall have established documented procedures to backup Medi-Cal PII to maintain retrievable exact copies of Medi-Cal PII.
 - 2. The documented backup procedures shall contain a schedule which includes incremental and full backups.
 - 3. The procedures shall include storing backups containing Medi-Cal PII offsite.
 - 4. The procedures shall ensure an inventory of backup media. It is recommended that the County Department/Agency periodically test the data recovery process.

IX. PAPER DOCUMENT CONTROLS

- A. **Supervision of Data.** Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.
- B. **Data in Vehicles.** The County Department/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. A County

During the term of this Agreement, the County Department/Agency agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

A. Initial Notice to DHCS:

The County Department/Agency shall notify DHCS, by email, or alternatively, by telephone if email is unavailable, of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII or potential loss of Medi-Cal PII. When making notification, the following applies:

1. If a suspected security incident involves Medi-Cal PII provided or verified by SSA, the County Department/Agency shall **immediately** notify DHCS upon discovery. *For more information on SSA data, please see the Definition section of this Agreement.*
2. If a suspected security incident does not involve Medi-Cal PII provided or verified by SSA, the County Department/Agency shall notify DHCS **within one working day** of discovery.

If it is unclear if the security incident involves SSA data, the County Department/Agency shall immediately report the incident upon discovery.

A County Department/Agency shall notify DHCS of all personal information, as defined by California Civil Code Section 1798.3(a), that may have been accessed, used, or disclosed in any suspected security incident or breach, including but not limited to case numbers.

Notice shall be made using the DHCS Privacy Incident Report (PIR) form, including all information known at the time. The County Department/Agency shall use the most current version of this form, which is available on the DHCS Privacy Office website at:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx>.

All PIRs and supporting documentation are to be submitted to DHCS via email using the "DHCS Breach and Security Incidents Reporting" contact information found below in Subsection F.

A breach shall be treated as discovered by the County Department/Agency as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the County Department.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, the County Department/Agency shall take:

1. Prompt action to mitigate any risks or damages involved with the occurrence and to protect the operating environment; and
2. Any action pertaining to such occurrence required by applicable Federal and State laws and regulations.

B. **Investigation and Investigative Report.** The County Department/Agency shall immediately investigate breaches and security incidents involving Medi-Cal PII. If the initial PIR was submitted incomplete and if new or updated information is available, submit an updated PIR to DHCS within **72 hours of the discovery**. The updated PIR shall include any other applicable information related to the breach or security incident known at that time.

C. **Complete Report.** If all of the required information was not included in either the initial report or the investigation PIR submission, then a separate complete report shall be submitted **within ten working days of the discovery**. The Complete Report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law. The report shall also include a CAP that shall include, at minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If DHCS requests additional information related to the incident, the County Department/Agency shall make reasonable efforts to provide DHCS with such information. If necessary, the County Department/Agency shall submit an updated PIR with revisions and/or additional information after the Completed Report has been provided. DHCS will review and determine whether a breach occurred and whether individual notification is required. DHCS will maintain the final decision making over a breach determination.

- D. **Notification of Individuals.** When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their Medi-Cal PII, the County Department/Agency shall give the notice, subject to the following provisions:
1. If the cause of the breach is attributable to the County Department/Agency or its subcontractors, agents or vendors, the County Department/Agency shall pay any costs of such notifications, as well as any and all costs associated with the breach. If the cause of the breach is attributable to DHCS, DHCS shall pay any costs associated with such notifications, as well as any costs associated with the breach.

If there is any question as to whether DHCS or the County Department/Agency is responsible for the breach, DHCS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs;

2. All notifications (regardless of breach status) regarding beneficiaries' Medi-Cal PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than **60 calendar days** from discovery;
3. The DHCS Privacy Office shall approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. If notifications are distributed without DHCS review and approval, secondary follow-up notifications may be required; and
4. DHCS may elect to assume responsibility for such notification from the County Department/Agency.

E. Responsibility for Reporting of Breaches when Required by State or Federal Law. If the cause of a breach of Medi-Cal PII is attributable to the County Department/Agency or its agents, subcontractors or vendors, the County Department/Agency is responsible for all required reporting of the breach. If the cause of the breach is attributable to DHCS, DHCS is responsible for all required reporting of the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS and the County Department/Agency shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

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

DHCS Breach and Security Incident Reporting
Department of Health Care Services Office of HIPAA Compliance 1501 Capitol Avenue, MS 4721 P.O. Box 997413 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (866) 866-0602 <i>The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.</i>

XI. DHCS PSA CONTACTS

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

PSA Inquires and Questions
Department of Health Care Services Medi-Cal Eligibility Division 1501 Capitol Avenue, MS 4607 P.O. Box 997417 Sacramento, CA 95899-7417 Email: countypsa@dhcs.ca.gov

XII. COMPLIANCE WITH SSA AGREEMENT

The County Department/Agency agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CHHS), in the Information Exchange Agreement (IEA) between SSA and DHCS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are hereby incorporated into this Agreement (Exhibit A) and available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

If SSA changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to County Welfare Directors Association (CWDA) as well as the proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, DHCS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, DHCS will supply copies of the changed agreement to the CWDA and the County Departments/Agency, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date, it shall submit a CAP to DHCS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential County Department/Agency resource issues may be discussed with DHCS through a collaborative process in developing their CAP.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section XI of this Agreement.

XIII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County Department/Agency agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and DHCS, which is hereby incorporated into this Agreement (Exhibit B) and available upon request. If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

If DHS-USCIS changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to CWDA as well as the DHCS proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the 30-day period, DHCS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once a target date for compliance is determined by DHS-USCIS,

DHCS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by DHS-USCIS. If the County Department/Agency is not able to meet the DHS-USCIS compliance date, it shall submit a CAP to DHCS for review and approval at least thirty (30) days prior to the DHS-USCIS compliance date. Any potential County Department/Agency resource issues may be discussed with DHCS through a collaborative process in developing their CAP.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section XI of this Agreement.

XIV. COUNTY DEPARTMENT'S/AGENCY'S AGENTS, SUBCONTRACTORS, AND VENDORS

The County Department/Agency agrees to enter into written agreements with all agents, subcontractors and vendors that have access to County Department/Agency Medi-Cal PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the County Department/Agency with respect to Medi-Cal PII upon such agents, subcontractors, and vendors. These shall include, (1) restrictions on disclosure of Medi-Cal PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect Medi-Cal PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII be reported to the County Department/Agency. If the agents, subcontractors, and vendors of County Department/Agency access data provided to DHCS and/or CDSS by SSA or DHS-USCIS, the County Department/Agency shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors. If the County Department/Agency executed the HIPAA Amendment with DHCS, the HIPAA Amendment and Exhibit C will need to be incorporated when applicable. County Departments/Agencies who would like assistance or guidance with this requirement are encouraged to contact DHCS via the PSA inbox at CountyPSA@dhcs.ca.gov.

XV. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the County Department/Agency agrees to assist DHCS in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the County Department/Agency, with reasonable notice from DHCS. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The County Department/Agency agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the DHCS

Privacy Office and DHCS Information Security Office in writing, or to enter into a written CAP with DHCS containing deadlines for achieving compliance with specific provisions of this Agreement.

XVI. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XVII. AMENDMENT OF AGREEMENT

DHCS and the County Department/Agency acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. Upon request by DHCS, the County Department/Agency agrees to promptly enter into negotiations with DHCS concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. In addition to any other lawful remedy, DHCS may terminate this Agreement upon 30 days written notice if the County Department/Agency does not promptly agree to enter into negotiations to amend this Agreement when requested to do so, or does not enter into an amendment that DHCS deems necessary.

XVIII. TERMINATION

- A. This Agreement shall terminate on September 1, 2022, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement; through an executed written amendment. County Department/Agency requests for an extension shall be justified and approved by DHCS and limited to no more than a six (6) month extension.
- B. **Survival:** All provisions of this Agreement that provide restrictions on disclosures of Medi-Cal PII and that provide administrative, technical, and physical safeguards for the Medi-Cal PII in the County Department/Agency's

possession shall continue in effect beyond the termination or expiration of this Agreement, and shall continue until the Medi-Cal PII is destroyed or returned to DHCS.

XIX. TERMINATION FOR CAUSE

Upon DHCS' knowledge of a material breach or violation of this Agreement by the County Department/Agency, DHCS may provide an opportunity for the County Department/Agency to cure the breach or end the violation and may terminate this Agreement if the County Department/Agency does not cure the breach or end the violation within the time specified by DHCS. This Agreement may be terminated immediately by DHCS if the County Department/Agency has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department/Agency shall return or destroy all Medi-Cal PII in accordance with Section VII, above. The provisions of this Agreement governing the privacy and security of the Medi-Cal PII shall remain in effect until all Medi-Cal PII is returned or destroyed and DHCS receives a certificate of destruction.

XX. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on September 1, 2019.

For the County of Yuba
Department/Agency of Health and Human Services



(Signature)

November 12, 2019

(Date)

Mike Leahy

(Name)

Chair, Yuba County Board of Supervisors

(Title)

For the Department of Health Care Services,

Richard Figueroa
(Signature)

11/24/19
(Date)

Richard Figueroa
(Name)

Acting Director
(Title)

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff from DHCS by using the contact information listed in Section XI of this Agreement.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and DHCS
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff from DHCS by using the contact information listed in Section XI of this Agreement.

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

ATTACHMENT D

MOU-19-6080
CDSS/County of Yuba Health & Human Services Department

554-2019

2019 PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Social Services and the
County of Yuba

Department/Agency of Health and Human Services

PREAMBLE

The California Department of Social Services (CDSS) and the
County of Yuba

Department/Agency of Health and Human Services

enter into this Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Social Security Administration (SSA), Medi-Cal Eligibility Data System (MEDS) and Applicant Income and Eligibility Verification System (IEVS) Personally Identifiable Information (PII), covered by this Agreement and referred to hereinafter as PII, that the counties access through CDSS and the Department of Health Care Services (DHCS). This Agreement covers the following programs:

- CalFresh;
- California Food Assistance Program (CFAP);
- California Work Opportunity and Responsibility to Kids Program (CalWORKs);
- Cash Assistance Program for Immigrants (CAPI);
- Entrant Cash Assistance (ECA)/Refugee Cash Assistance (RCA);
- Foster Care (FC) (eligibility);
- Kinship Guardianship Assistance Program (Kin-GAP) (eligibility);
- Federal Guardianship Assistance Program (Fed-GAP) (eligibility);
- General Assistance/General Relief (GA/GR); and
- Trafficking and Crime Victims Assistance Program (TCVAP).

The CDSS has an Inter-Agency Agreement (IAA) with DHCS that allows CDSS and local county agencies to access SSA and MEDS data in order to Assist in the Administration of the Program for the programs listed above. The IAA requires that CDSS may only share SSA and MEDS data if its contract with the entity with whom it intends to share the data reflects the entity's obligations under the IAA.

v2019 06 24
Page 1 of 24

The County Department/Agency utilizes SSA and MEDS data in conjunction with other system data in order to Assist in the Administration of the Program for the programs listed above.

This Agreement covers the

County of Yuba

Department/Agency of Health and Human Services

and its staff (County Workers), who access, use, or disclose PII covered by this Agreement, to assist in the administration of programs.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. **"Assist in the Administration of the Program"** means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.
2. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
3. **"County Worker"** means those county employees, contractors, subcontractors, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.
4. **"PII"** is personally identifiable information directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of the programs, which can be used alone, or in conjunction with any other reasonably available information to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including, but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

5. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.
6. **"Secure Areas"** means any area where:
 - a. County Workers assist in the administration of their program;
 - b. County Workers use or disclose PII; or
 - c. PII is stored in paper or electronic format.
7. **"SSA-provided or verified data (SSA data)"** means:
 - a. Any information under the control of the Social Security Administration (SSA) provided to CDSS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or;
 - b. Any information provided to CDSS, including a source other than SSA, but in which CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

5. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.
6. **"Secure Areas"** means any area where:
 - a. County Workers assist in the administration of their program;
 - b. County Workers use or disclose PII; or
 - c. PII is stored in paper or electronic format.
7. **"SSA-provided or verified data (SSA data)"** means:
 - a. Any information under the control of the Social Security Administration (SSA) provided to CDSS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or;
 - b. Any information provided to CDSS, including a source other than SSA, but in which CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

AGREEMENTS

CDSS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

- A. County Workers may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et seq. and Welfare and Institutions Code section 10850 or as authorized or required by law. Disclosures required by law or that are made with the explicit written authorization of the client are allowable. Any other use or disclosure of PII requires the express approval in writing of CDSS. No County Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- B. Pursuant to this Agreement, County Workers may only use PII to assist in administering their respective programs.
- C. Access to PII shall be restricted to County Workers who need to perform their official duties to assist in the administration of their respective programs.
- D. County Workers who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

The County Department/Agency agrees to advise County Workers who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department/Agency shall implement the following personnel controls:

- A. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:
 - 1. Provide initial privacy and security awareness training to each new County Worker within thirty (30) days of employment;
 - 2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three (3) or more security reminders per year are recommended;

3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed; and
4. Retain training records for a period of three (3) years after completion of the training.

B. *Employee Discipline*

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

- C. *Confidentiality Statement***. Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years, or five (5) years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

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

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

D. *Background Screening*

1. Conduct a background screening of a County Worker before they may access PII.
2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3. The County Department/Agency shall retain each County Worker's background screening documentation for a period of three (3) years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

To ensure compliance with the privacy and security safeguards in this Agreement the County Department/Agency shall perform the following:

- A. Conduct periodic privacy and security reviews of work activity by County Workers, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.
- B. The periodic privacy and security reviews shall be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of their program, and the use or disclosure of PII.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department/Agency agrees to:

- A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.
- B. Provide CDSS with applicable contact information for these designated individuals by emailing CDSS at cdsspsa@dss.ca.gov. Any changes to this information should be reported to CDSS within ten (10) days.
- C. Assign County Workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

The County Department/Agency shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The County Department/Agency agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

- A. Secure all areas of the County Department/Agency facilities where County Workers assist in the administration of their program and use, disclose, or store PII.
- B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:

1. Properly coded key cards
 2. Authorized door keys
 3. Official identification
- C. Issue identification badges to County Workers.
- D. Require County Workers to wear these badges where PII is used, disclosed, or stored.
- E. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.
- F. Ensure there are security guards or a monitored alarm system at all times at the County Department/Agency facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.
- G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized County Workers. Visitors to the data center area shall be escorted at all times by authorized County Workers.
- H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County Department/Agency and non-County Department/Agency functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.
- I. The County Department/Agency shall have policies based on applicable factors that include, at a minimum, a description of the circumstances under which the County Workers can transport PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles shall include provisions in its policies to ensure that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

- J. The County Department/Agency shall have policies that indicate County Workers are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.
- K. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

VI. TECHNICAL SECURITY CONTROLS

- A. **Workstation/Laptop Encryption.** All workstations and laptops, which use, store and/or process PII, shall be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- B. **Server Security.** Servers containing unencrypted PII shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- C. **Minimum Necessary.** Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.
- D. **Mobile Device and Removable Media.** All electronic files, which contain PII, shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption shall be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- E. **Antivirus Software.** All workstations, laptops and other systems, which process and/or store PII, shall install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.
- F. **Patch Management.**
 - 1. All workstations, laptops and other systems, which process and/or store PII, shall have critical security patches applied, with system reboot if necessary.

2. There shall be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
3. At a maximum, all applicable patches deemed as critical shall be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, shall have compensatory controls implemented to minimize risk.

G. *User IDs and Password Controls.*

1. All users shall be issued a unique user name for accessing PII.
2. Username shall be promptly disabled, deleted, or the password changed within, at most, twenty-four (24) hours of the transfer or termination of an employee. Note: Twenty-four (24) hours is defined as one (1) working day.
3. Passwords are not to be shared.
4. Passwords shall be at least eight (8) characters.
5. Passwords shall be a non-dictionary word.
6. Passwords shall not be stored in readable format on the computer or server.
7. Passwords shall be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less. Non-expiring passwords are permitted when in full compliance with NIST SP 800-63B Authenticator Assurance Level (AAL) 2.
8. Passwords shall be changed if revealed or compromised.

9. Passwords shall be composed of characters from at least three (3) of the four (4) of the following groups from the standard keyboard:
 - a. Upper case letters (A-Z)
 - b. Lower case letters (a-z)
 - c. Arabic numerals (0-9)
 - d. Special characters (!,@,#, etc.)
- H. **User Access.** In conjunction with CDSS and DHCS, County Department/Agency management should exercise control and oversight over the authorization of individual user access to SSA data via, MEDS, IEVS, and over the process of issuing and maintaining access control numbers, IDs, and passwords.
- I. **Data Destruction.** When no longer needed, all PII shall be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.
- J. **System Timeout.** The systems providing access to PII shall provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
- K. **Warning Banners.** The systems providing access to PII shall display a warning banner stating, at a minimum:
 1. Data is confidential;
 2. Systems are logged;
 3. System use is for business purposes only, by authorized users; and
 4. Users shall log off the system immediately if they do not agree with these requirements.
- L. **System Logging.**
 1. The systems that provide access to PII shall maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.

2. The audit trail shall:
 - a. Be date and time stamped;
 - b. Log both successful and failed accesses;
 - c. Be read-access only; and
 - d. Be restricted to authorized users of the audit trail.
 3. If PII is stored in a database, database logging functionality shall be enabled.
 4. Audit trail data shall be archived for at least three (3) years from the occurrence.
- M. **Access Controls.** The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.
- N. **Transmission Encryption.**
1. All data transmissions of PII outside of a secure internal network shall be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256-bit encryption be used.
 2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
 3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.
- O. **Intrusion Prevention.** All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, shall be protected by an intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. *System Security Review.*

1. The County Department/Agency shall ensure audit control mechanisms are in place.

2. All systems processing and/or storing PII shall have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
 3. Reviews should include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing PII shall have a process or automated procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing PII shall have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.
- D. **Anomalies.** When the County Department/Agency or DHCS suspects MEDS usage anomalies, the County Department/Agency will work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to CDSS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

- A. **Emergency Mode Operation Plan.** The County Department/Agency shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours. It is recommended that County Department/Agency conduct periodic disaster recovery testing, including connectivity exercises conducted with DHCS and CDSS, if requested.
- B. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, shall include environmental protection such as cooling, power, and fire prevention, detection, and suppression; and appropriate protection from other threats, including but not limited to flood, earthquake, and terrorism.
- C. **Data Backup and Recovery Plan.**
1. The County Department/Agency shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
 2. The documented backup procedures shall contain a schedule which includes incremental and full backups.

3. The procedures shall include storing backups containing PII offsite.
4. The procedures shall ensure an inventory of backup media.
5. The County Department/Agency shall have established documented procedures to recover PII data.
6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
7. It is recommended that the County Department/Agency periodically test the data recovery process.

IX. PAPER DOCUMENT CONTROLS

- A. ***Supervision of Data.*** The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.
- B. ***Data in Vehicles.*** The County Department/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII to be left unattended in a vehicle overnight or for other extended periods of time.
- C. ***Public Modes of Transportation.*** The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.
- D. ***Escorting Visitors.*** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.
- E. ***Confidential Destruction.*** PII shall be disposed of through confidential means, such as cross cut shredding or pulverizing.
- F. ***Removal of Data.*** The PII shall not be removed from the premises of County Department/Agency except for identified routine business purposes or with express written permission of CDSS.

G. Faxing.

1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. Mailing.

1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the County Department/Agency obtains prior written permission from CDSS to use another method.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the County Department/Agency agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

A. *Initial Notice to DHCS:*

The County Department/Agency will provide initial notice to DHCS by email, or alternatively, by telephone if email is unavailable, of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII with a copy to CDSS. The DHCS is acting on behalf of CDSS for purposes of receiving reports of privacy and information security incidents and breaches. The County Department/Agency agrees to perform the following incident reporting to DHCS:

1. If a suspected security incident involves PII provided or verified by SSA, the County Department/Agency shall immediately notify DHCS upon discovery. For more information on SSA data, please see the Definition section of this Agreement.

2. If a suspected security incident does not involve PII provided or verified by SSA, the County Department/Agency shall notify DHCS within one (1) working day of discovery.

If it is unclear if the security incident involves SSA data, the County Department/Agency shall immediately report the incident upon discovery.

A County Department/Agency shall notify DHCS of all personal information, as defined by California Civil Code Section 1798.3(a), that may have been accessed, used, or disclosed in any suspected security incident or breach, including but not limited to case numbers.

Notice shall be made using the DHCS Privacy Incident Report (PIR) form, including all information known at the time. The County Department/Agency shall use the most current version of this form, which is available on the DHCS Privacy Office website at:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx>.

All PIRs and supporting documentation are to be submitted to DHCS via email using the "DHCS Breach and Security Incidents Reporting" contact information found below in Subsection F.

A breach shall be treated as discovered by the County Department/Agency as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the County Department/Agency.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the County Department/Agency shall take:

1. Prompt action to mitigate any risks or damages involved with the occurrence and to protect the operating environment; and
 2. Any action pertaining to such occurrence required by applicable Federal and State laws and regulations.
- B. Investigation and Investigative Report. The County Department/Agency shall immediately investigate breaches and security incidents involving PII. If the initial PIR was submitted incomplete and if new or updated information is available, submit an updated PIR to DHCS within seventy-two (72) hours of the discovery. The updated PIR shall include any other applicable information related to the breach or security incident known at that time.

- C. **Complete Report.** If all of the required information was not included in either the initial report or the investigation PIR submission, then a separate complete report shall be submitted within ten working days of the discovery. The Complete Report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law. The report shall also include a Corrective Action Plan (CAP) that shall include, at minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If DHCS requests additional information related to the incident, the County Department/Agency shall make reasonable efforts to provide DHCS with such information. If necessary, the County Department/Agency shall submit an updated PIR with revisions and/or additional information after the Completed Report has been provided. DHCS will review and determine whether a breach occurred and whether individual notification is required. DHCS will maintain the final decision making over a breach determination.

- D. **Notification of Individuals.** When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County Department/Agency shall give the notice, subject to the following provisions:
1. If the cause of the breach is attributable to the County Department/Agency or its subcontractors, agents or vendors, the County Department/Agency shall pay any costs of such notifications, as well as any and all costs associated with the breach. If the cause of the breach is attributable to CDSS, CDSS shall pay any costs associated with such notifications, as well as any costs associated with the breach. If there is any question as to whether CDSS or the County Department/Agency is responsible for the breach, CDSS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs;

2. All notifications (regardless of breach status) regarding beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event, later than sixty (60) calendar days from discovery;
 3. The CDSS Information Security and Privacy Bureau shall approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. If notifications are distributed without CDSS review and approval, secondary follow-up notifications may be required; and
 4. CDSS may elect to assume responsibility for such notification from the County Department/Agency.
- E. **Responsibility for Reporting of Breaches when Required by State or Federal Law.** If the cause of a breach is attributable to the County Department/Agency or its agents, subcontractors or vendors, the County Department/Agency is responsible for all required reporting of the breach. If the cause of the breach is attributable to CDSS, CDSS is responsible for all required reporting of the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS (if the breach involves MEDS or SSA data), CDSS, and the County Department/Agency shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.
- F. **CDSS and DHCS Contact Information.** The County Department/Agency shall utilize the below contact information to direct all notifications of breach and security incidents to CDSS and DHCS. CDSS reserves the right to make changes to the contact information by giving written notice to the County Department/Agency. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

CDSS Information Security and Privacy Bureau	DHCS Breach and Security Incident Reporting
<p>California Department of Social Services Information Security and Privacy Bureau 744 P Street, MS 9-9-70 Sacramento, CA 95814-6413</p> <p>Email: iso@dss.ca.gov</p> <p>Telephone: (916) 651-5558</p> <p><i>The preferred method of communication is email, when available. Do not include any PII unless requested by CDSS.</i></p>	<p>Department of Health Care Services Office of HIPAA Compliance 1501 Capitol Avenue, MS 4721 P.O. Box 997413 Sacramento, CA 95899-7413</p> <p>Email: incidents@dhcs.ca.gov</p> <p>Telephone: (866) 866-0602</p> <p><i>The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.</i></p>

XI. COMPLIANCE WITH SSA AGREEMENT

The County Department/Agency agrees 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 Agreement (IEA) between SSA and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are hereby incorporated into this Agreement (Exhibit A) and available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If SSA changes the terms of its agreement(s) with CDSS, CDSS will, as soon as reasonably possible after receipt, supply copies to the County Welfare Directors Association (CWDA) as well as the proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, CDSS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date, it shall submit a CAP to CDSS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential County Department/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County Department/Agency agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS, which is hereby incorporated into this Agreement (Exhibit B) and available upon request. If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If DHS-USCIS changes the terms of its agreement(s) with CDSS, CDSS will, as soon as reasonably possible after receipt, supply copies to CWDA as well as the CDSS proposed target date for compliance. For a period of thirty (30) days, CDSS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, CDSS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once a target date for compliance is determined by DHS-USCIS, CDSS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by DHS-USCIS. If a County Department/Agency is not able to meet the DHS-USCIS compliance date, it shall submit a CAP to CDSS for review and approval at least thirty (30) days prior to the DHS-USCIS compliance date. Any potential County Department/Agency resource issues may be discussed with CDSS through a collaborative process in developing their CAP.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals by emailing CDSS at cdsspsa@dss.ca.gov.

XIII. COUNTY DEPARTMENT/AGENCY AGENTS, SUBCONTRACTORS, AND VENDORS

The County Department/Agency agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to County Department/Agency PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the County Department/Agency with respect to PII upon such agents, subcontractors, and vendors. These shall include, at a minimum, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the County Department/Agency. If the agents, subcontractors, and vendors of County Department/Agency access data provided to DHCS and/or CDSS by SSA or DHS-USCIS, the County Department/Agency shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

County Department/Agency(s) who would like assistance or guidance with this requirement are encouraged to contact CDSS via email at cdsspsa@dss.ca.gov.

XIV. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the County Department/Agency agrees to assist CDSS or DHCS (on behalf of CDSS) in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the County Department/Agency, with reasonable notice from CDSS or DHCS. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The County Department/Agency agrees to promptly remedy all violations of any provision of this Agreement and certify the same to CDSS in writing, or to enter into a written CAP with CDSS containing deadlines for achieving compliance with specific provisions of this Agreement.

XV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

XVI. AMENDMENT OF AGREEMENT

The CDSS and the County Department/Agency acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that an amendment to this Agreement may be required to ensure compliance with all data security and privacy procedures. Upon request by CDSS, the County Department/Agency agrees to promptly enter into negotiations with CDSS concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. In addition to any other lawful remedy, CDSS may terminate this Agreement upon thirty (30) days written notice if the County Department/Agency does not promptly agree to enter into negotiations to amend this Agreement when requested to do so, or does not enter into an amendment that CDSS deems necessary.

Each amendment shall be properly identified as Agreement No., Amendment No. (A-1, A-2, A-3, etc.) to identify the applicable changes to this Agreement, and be effective upon execution by the parties.

XVII. TERM OF AGREEMENT

The term of this agreement shall begin upon signature and approval of CDSS.

XVIII. TERMINATION

A. This Agreement shall terminate on **September 1, 2022**, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement; through an executed written amendment. County Department/Agency requests for an extension shall be justified and approved by CDSS and limited to no more than a six (6) month extension.

B. **Survival:** All provisions of this Agreement that provide restrictions on disclosures of PII and that provide administrative, technical, and physical safeguards for the PII in the County Department/Agency's possession shall continue in effect beyond the termination or expiration of this Agreement, and shall continue until the PII is destroyed or returned to CDSS.

XIX. TERMINATION FOR CAUSE

Upon CDSS' knowledge of a material breach or violation of this Agreement by the County Department/Agency, CDSS may provide an opportunity for the County Department/Agency to cure the breach or end the violation and may terminate this Agreement if the County Department/Agency does not cure the breach or end the violation within the time specified by CDSS. This Agreement may be terminated immediately by CDSS if the County Department/Agency has breached a material term and CDSS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department/Agency shall return or destroy all PII in accordance with Section VI, above. The provisions of this Agreement governing the privacy and security of the PII shall remain in effect until all PII is returned or destroyed and CDSS receives a certificate of destruction.

XX. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on September 1, 2019.

For the County of Yuba
Department/Agency of Health and Human Services



(Signature) November 12, 2019

(Date)

Mike Leahy Chair, Yuba County Board of Supervisors

(Name – Print or Type) (Title – Print or Type)

For the California Department of Social Services,



(Signature) 1/8/2020

(Date)

Simone Dumas Chief, Contracts & Purchasing Bureau


(Name – Print or Type) (Title – Print or Type)

RECOMMENDED FOR APPROVAL:
INFORMATION TECHNOLOGY



Paul LaValley, Chief Information Officer

APPROVED AS TO FORM:
MICHAEL J. CICCOTZI



County Counsel A. SULLIVAN, DEPUTY

RECOMMENDED FOR APPROVAL:



Jennifer Vasquez, Director
Yuba County Health and Human
Services Department

v2019 06 24
Page 23 of 24

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff from CDSS by emailing CDSS at cdsspsa@dss.ca.gov.

- Computer Matching and Privacy Protection Act Agreement between the SSA and California Health and Human Services Agency
- Information Exchange Agreement between SSA and CDSS (IEA-F and IEA-S)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA (TSSR)

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff by emailing CDSS at cdsspsa@dss.ca.gov.

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