STANISLAUS COUNTY COMMUNITY SERVICES AGENCY	Developed by/Date: Bernard Licata March 06, 2020	Page: 1 of 11	Number: 1.5
			Category: Administrative
	Reviewed by/Reviewed Date: CSA Exec Team 9/20/21	Replaces: 1.5	Distribution: All Staff

Title: Approved: 9/20/21

Privacy, Security & Safeguarding of Confidential, Protected & Personally Identifiable Information

Policy ☑ **Procedure** ☐ **Guideline** ☐

PURPOSE

To set policy and expectations for the Stanislaus County Community Services Agency (CSA) to comply with state and federal laws, regulations, policies, procedures, use agreements and training governing the privacy, security and safeguarding of Confidential, Protected, and Personally Identifiable Information.

DEFINITIONS

Administration of the Program means performing administrative functions on behalf of allowable programs such as determining or maintaining eligibility, enrollment, and collecting PII for such purposes to the extent such activities are permitted by law.

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.

Confidentiality is the concept of ensuring that information is observable only by those who are granted authorization to do so and possess a need-to-know and right-to-know business necessity.

Conflict of Interest is defined as a conflict between the personal interests and the official duties and responsibilities of a County Worker in a position of trust.

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.

PII is personally identifiable information directly obtained in the course of performing an administrative function 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.

Protected Information is any information or data other than PII that is collected, stored or accessed by County Workers and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local databases that are not accessible to the public.

Public Assistance refers to any public social service program, aid or service authorized and administered by CSA, its contractors, subcontractors, vendors or agents.

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.

Secure Area is a facility, or an area, a room, or a group of rooms, within a facility used by County Workers to administer programs, use or disclose PII, or store PII in electronic or paper format with both the physical, technological, and personnel security controls sufficient to protect PII and associated information systems.

SSA-provided or verified data (SSA data) means:

A. Any information under the control of the Social Security Administration (SSA) provided to CDSS or DHCS under the terms of an information exchange agreement with SSA or;

B. Any information provided to CDSS or DHCS, including a source other than SSA, but in which CDSS or DHCS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it.

POLICY

The Community Services Agency is committed to ensuring privacy, security and safeguarding against unauthorized access or use of Confidential, Protected or Personally Identifiable Information (PII) stored or used on any CSA computer system, database, electronic media, or paper file. This policy shall also apply to County Workers authorized to access data systems not owned or controlled by CSA. County Workers that require authorized access to Confidential, Protected or Personally Identifiable Information shall adhere to all applicable laws, orders, regulations, policies, procedures, MOUs, use agreements and training related to the privacy, security, access, use, viewing, modification, transmission, dissemination, release, storage, destruction and overall safeguarding of such information. Data is sourced

by the Social Security Administration (SSA), Medi-Cal Eligibility Data System (MEDS), and the Applicant Income and Eligibility Verification System (IEVS) for the limited purpose of assisting County Workers in the administration of authorized programs.
Any person within the jurisdiction of this policy who fails to comply with its provisions may be subject to civil or criminal sanctions, corrective action, discipline, or any combination thereof.

PROCEDURE

A. PERMISSIONS AND ACCESS

County Workers shall be required to complete an appropriate background screening, Privacy and Security Awareness training, and sign confidentiality statements prior to being granted access to Confidential, Protected, or PII.

1. County Workers shall comply with all applicable laws (California Department of Social Services MPP, Division 19: *Confidentiality of Information*, 45 CFR Part 164, 45 CFR § 205.50 et seq., 42 CFR § 431.300 et seq., California Welfare & Institutions Code §§ 10850 and 14100.2, and California Penal Code § 502), as well as orders, regulations, policies, procedures, use agreements and training to the extent it is necessary to perform their duties based upon the administration of public assistance.

2. County Workers granted access to, but not limited to CalSAWS, HMIS, CWS/CMS, CMIPS, LEAPS, and APS databases shall comply with all applicable laws, orders, regulations, policies, procedures, use agreements and training to the extent it is necessary to perform their duties.
3. County Worker Case Confidentiality

The following qualifies as a County Worker Confidential case:

a. Any County Worker who is an applicant, participant, recipient, or beneficiary of public assistance including foster care benefits, and who has access to Confidential, Protected, or PII controlled by CSA.

b. Any County Worker identified in, but not limited to CWS/CMS, CMIPS, LEAPS, HMIS, and APS databases.

c. Paid WEX/Community Service Program Customer placed at a CSA facility or placed off-site with access to the CSA CalSAWS system.

d. Safe at Home Customers
The supervisor or manager shall evaluate if the case qualifies as a County Worker Confidential Case. Cases deemed to be confidential in the CalSAWS database will be marked by the authorized supervisor, manager, or CalSAWS Security Specialist with the appropriate confidentiality type.

Cases deemed to be confidential that reside in other databases such as HMIS,

CWS/CMS, CMIPS, LEAPS, and APS shall comply with statutory, regulatory, and County policies and procedures for identifying the appropriate confidentiality type.

4. Conflict of Interest

In order to avert potential conflicts of interest, County Workers shall:

a. Disclose to their respective supervisor/manager if they are a current applicant, participant, recipient or beneficiary of public assistance, including foster care benefits or if they become an applicant, recipient, or beneficiary in the future while employed by the County and assigned to work at CSA immediately upon employment or application for a public assistance program.

b. Identify others they know who are applicants, participants, beneficiaries or recipients of public assistance, such as a personal friend, relative, co-worker, neighbor, business associate, or anyone they have personal knowledge of that could lead to a conflict of interest to their respective supervisor/manager as soon as they become aware of such potential conflict of interest.

c. Identify others they know who are found in databases such as HMIS, CWS/CMS, CMIPS, LEAPS, and APS, such as a personal friend, relative, co-worker, neighbor, business associate, or anyone they have personal knowledge of that could lead to a conflict of interest to their respective supervisor/manager as soon as they become aware of such potential conflict of interest.

d. The supervisor or manager shall evaluate the reported or discovered conflict of interest to determine if the affected County Worker should be prohibited from accessing a particular case and if the case qualifies as a County Worker confidential case.

5. County Workers **SHALL NOT**:

a. Access, use, disclose, discuss, publish, permit or cause unauthorized access, use, or publication of any Confidential, Protected or PII pertaining to any applicant or recipient of public assistance without explicit agency, applicant or recipient authorization and a legitimate need-to-know and right-to-know business necessity.

b. Access either personally or through other unauthorized means, any information regarding their own case record or personal information, a personal friend, relative, co-worker, neighbor, business associate, or anyone they have personal knowledge of that could lead to a conflict of interest.

c. Use county work time or general work areas to receive any personal case related services if they are a CSA customer.

6. Allowances shall be made for persons who serve on multi-disciplinary teams, as defined in California Welfare & Institutions Code §10850.1, to disclose to one another information which is relevant to the services provided to any person(s) under the terms of this policy.

B. COMPLIANCE WITH SSA and DEPARTMENT OF HOMELAND SECURITY AGREEMENTS

1. County Workers shall comply with applicable privacy and security requirements in:

   a. Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS),

   b. Information Exchange Agreement (IEA) between SSA and CDSS,

   c. Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Information with SSA (TSSR), and

   d. Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the CDSS.

2. If any conflicts between a privacy and security standard in the CMPPA, IEA, TSSR, or CMA and a standard in an existing Privacy and Security Agreement between CSA and the CDSS or DHCS exist, the standard that provides the greatest protection to PII shall apply.

C. PHYSICAL SECURITY CONTROLS

1. All Confidential, Protected and PII shall be used, disclosed, and stored in a secure area that is physically safe from access by unauthorized persons at all times and such areas shall be restricted to only allow access to authorized County Workers.

2. County Workers are required to wear County or other authorized issued identification badges at all times while inside any facility where Confidential, Protected, and PII is used, disclosed, and stored in a manner that is clearly visible to others.

3. Work area physical security requirements include:

   a. PII shall not be left unattended or unsecured on desktops, areas open or viewable by the public, on copiers, printers, in conference rooms, interview rooms, or other places where information may be compromised.

b. PII stored in any Agency computer system, including but not limited to CalSAWS, CWS/CMS, CMIPS, LEAPS, APS, HMIS, managed or non-managed desktop or laptop computers or devices, and various other databases shall not be left unattended for any length of time without the user logging off or powering down the device.

c. Store all paper records with PII in locked file cabinets, shelves, file rooms, desks, or offices at all times at facilities and areas that are not securely segregated from other County or non-County Departments.

d. PII shall not be verbally transmitted when it can be overheard by unauthorized persons.

e. Visitors to any areas where PII is used, stored, disclosed, or processed must be escorted at all times by authorized staff.

4. Transporting PII in Vehicles and Public Modes of Transportation

a. PII may only be transported if there is a legitimate business need including, but not limited to home visits or delivery for proper storage, sanitation, or destruction.

b. PII must remain in the possession and control of authorized persons while in transit and may not be left unattended for any length of time on airplanes, buses, trains, or other conveyances except an automobile under the control of an authorized person.

c. If PII must be left unattended in an automobile, it must be stored and locked in an area not visible to others such as a glove box, trunk, or other secure storage container.

d. PII shall not be left unattended in an automobile overnight or for any period that exceeds four hours.

D. TECHNICAL SECURITY CONTORLS

1. User IDs and Password Controls

a. Are not to be shared.

b. Passwords shall be at least eight (8) characters, but shall be transitioned to the CSA expectation of passphrases with at least 14 characters in length.

c. Shall not be stored in readable format on the computer or server and shall not be written on post-it notes, or paper accessible to others.

d. Passwords shall be changed if revealed or compromised.

e. Passwords shall be composed of characters from at least three (3) of the four (4) of the following groups from the standard keyboard:

1. Upper case letters (A-Z)

2. Lower case letters (a-z)

3. Arabic numerals (0-9)

4. Special characters (@, #, $, etc.)

2. Minimum Necessary Information

a. Only the minimum necessary amount of Confidential, Protected, or PII required to perform business functions may be accessed, copied, downloaded or exported.

3. Encryption

a. All data transmissions of PII outside of the CSA secure internal network shall be encrypted including, but not limited to email, file transfer and website access.

b. All electronic files that contain PII shall be encrypted when stored on any mobile device or removable media.

E. PAPER DOCUMENT CONTROLS

1. Printing of Data

a. PII should not be printed unless required by a legitimate business need and utilizing only the minimum amount of PII required to perform a necessary business function.

b. In cases where a paper file exists and there is no database or limited database, the paper file may be accessed to perform a necessary business function. One existing example is CWS legal files that consist of a complete paper file and limited database information.

2. Supervision of Data

a. PII in paper form must not be left unattended at any time unless it is locked in a file cabinet, file room, desk, office, or otherwise secure space. Unattended means that information may be observed by an individual not authorized to access the information such as janitorial staff, customers, or visitors.

3. Facsimile of Data

    a. Fax machines used to transmit PII must be in secure areas and not be left unattended while sending a fax.

    b. All faxes must contain a confidentiality statement notifying persons receiving the faxes in error to destroy them and notify the sender.

    c. Fax numbers must be verified with the intended recipient before sending the fax.

4. Mailing Data

    a. Mail that contains PII must be sealed and secured from damage or inappropriate viewing of PII to the best extent possible.

    b. Mail that includes 500 or more individually identifiable records containing PII in a single package must be sent using a tracked mailing method that includes verification of delivery and receipt.

5. Removal of Data from Premises

    a. PII shall not be removed from the premises where it is generated or stored except for authorized, legitimate, and necessary business purposes or with express written permission of the CDSS.

6. Proper Handling and Confidential Destruction of Data

    a. All PII that is no longer needed must be cleared, purged, or destroyed.

    b. PII should be deposited in secure shred bins unless sourced from MEDS, IRS, or the DOJ.

    c. PII sourced from MEDS, IRS, or DOJ shall be pulverized utilizing approved agency cross-shredders under the supervision of authorized County Workers.

F. REPORTING AND INVESTIGATION OF BREACHES OF PII

1. Duty to Report Breaches of Security Data that Contains PII

    a. California Civil Code §§ 1798 et seq. requires a state agency that owns or licenses computerized data that includes PII MUST disclose any breach of security of the data to any resident of the state whose unencrypted PII was, or is, reasonably believed to have been acquired by an unauthorized person.

2. Investigation and the Investigative Report

a. Breaches and security incidents involving PII shall be investigated immediately upon discovery.

b. The supervisor or manager assigned to conduct the investigation shall prepare an investigative report on the Privacy Incident Report (PIR) form.

c. If the initial PIR is submitted incomplete, a new or updated report must be sent within seventy-two (72) hours of the discovery and include any other applicable information related to the breach or security incident known at that time.

d. If the new or updated report remains incomplete, then a separate complete report must be submitted within ten (10) business days of the discovery.

3. County Worker Staff Responsibilities

   a. Any County Worker who discovers a breach of data or security incident that contains PII shall immediately notify his or her supervisor or manager.

   b. If the breach of data or security incident is attributed to a contractor, sub-contractor, vendor, or agent, such staff shall also immediately notify the Quality or Program Integrity Manager of CSA.

   c. Any County Worker who discovers a breach shall explain how the breach came to his or her attention, the circumstances of how the breach occurred if known, and provide as much factual information as possible (names, dates, times, circumstances, etc.).

4. Supervisor Responsibilities

   a. Once the supervisor is apprised of a breach or security incident, he or she must verify whether in fact the circumstances meet the definition of a privacy breach.

   b. Take immediate steps to recover the breached data and to mitigate any further breaches.

   c. Gather as many facts as possible to identify who, what, when, where, why, and how of the incident.

   d. Fill out a Privacy Incident Report (PIR) according to instructions found under the Privacy Incident Report on the Agency intranet.

   e. The initial PIR should be completed and sent via email to the Quality Manager by 10:00 AM the next business day even if all the information is not available.

f. The supervisor of the employee who is responsible for the breach will conduct the investigation into the facts and record such on the PIR unless otherwise assigned by the responsible manager or Quality Manager.

g. The final PIR must be submitted to the Quality Manager via email once the investigation is complete and must include mitigation and corrective action plans.

5. Manager Responsibilities

   a. Provide oversight to ensure there are processes in place to discover and report privacy breaches.

   b. Ensure privacy breach policy and procedures are correctly followed.

   c. Assume supervisor responsibilities in the event a supervisor is responsible for the breach.

   d. Coordinate the privacy breach investigation.

   e. Review work processes and procedures to help formulate an appropriate Corrective Action Plan aimed at mitigating future privacy breaches.

   f. Conference with the supervisor, Human Resources Manager and Assistant Director to determine appropriate disciplinary action such as training and/or other sanctions that align with the County progressive discipline policy.

   g. Execute the Corrective Action Plan.

   h. Ensure the Corrective Action Plan and completed dates are reflected in the PIR and the Quality Manager in the Program Integrity section is sent all updates via email by 10:00 AM the next business day.

6. Program Integrity and Quality Manager Responsibilities

   a. Facilitate communication and oversight of privacy breach procedures.

   b. Offer guidance and assistance to supervisors and/or managers to identify, investigate, and report privacy breach incidents.

   c. Liaison and report breaches to the Privacy Officer and/or Information Security Officer of the California Department of Health Care Services (DHCS) as required by agreement.

   d. Examine the nature and scope of the breach and consult with DHCS to assure CSA takes appropriate courses of action.

e. Track investigations, issue report numbers, prepare client notices, and file all documentation of the breach as required by the DHCS.

f. Conference with managers and the CSA leadership to identify patterns and frequency of privacy breaches to identify mitigation strategies and corrective actions.

g. Assess and update privacy breach training as necessary to comply with changes in the law and pursuant to agreements with state and federal agencies.

G. COUNTY CONTRACTORS, SUBCONTRACTORS, VENDORS AND AGENTS

1. CSA shall enter into written agreements with all contractors, subcontractors, vendors and agents that have access to CSA PII. The agreements will impose the same terms and conditions with respect to the privacy, security, and safeguarding of Confidential, Protected, or PII contained in this policy.

2. All proposed privacy, security, and safeguarding agreements or amendments shall be reviewed by designated managers and County Counsel before being sent to the Director or his/her designee for final review and signature.

3. Privacy Security Agreement exhibits shall be incorporated into each subcontract or sub-award with contractors, subcontractors, vendors and agents if access is granted to data provided to DHCS and/or CDSS by SSA or DHS-USCIS.