

January 17, 2020

CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

EXECUTIVE SUMMARY

ALL COUNTY LETTER NO. 20-02

This All County Letter (ACL) will provide counties guidelines related to the security and privacy of In-Home Supportive Services program (IHSS) data related to implementing any new systems or ancillary tools that utilize data from the IHSS Case Management, Information and Payrolling System (CMIPS). This ACL will also outline the process for submitting documentation to the California Department of Social Services (CDSS) for review of the new systems or tools.



KIM JOHNSON
DIRECTOR

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



GAVIN NEWSOM
GOVERNOR

January 17, 2020

ALL COUNTY LETTER (ACL) NO. 20-02

TO: ALL COUNTY WELFARE DIRECTORS
ALL IHSS PROGRAM MANAGERS

SUBJECT: **COUNTY RESPONSIBILITY TO SECURE DATA RELATED TO
THE IN-HOME SUPPORTIVE SERVICES PROGRAM AND CASE
MANAGEMENT, INFORMATION AND PAYROLLING SYSTEM
BY NEW COUNTY SYSTEMS, APPLICATIONS OR ANCILLARY
TOOLS**

REFERENCE: [GOVERNMENT CODE SECTION 11015.5; WELFARE AND
INSTITUTIONS CODE SECTION 10850; CALIFORNIA CIVIL
CODE SECTION 1798.3\(a\)](#)

The purpose of this ACL is to provide counties with information, direction and expectations relating to the responsibilities for securing the confidentiality of data related to the In-Home Supportive Services (IHSS) Program in accordance with State and Federal guidelines. In addition, this ACL provides direction on a process for informing the California Department of Social Services (CDSS) when counties implement new systems, applications, and/or ancillary tools that will interface directly with data from the Case Management, Information and Payrolling System (CMIPS). These processes will be collectively referred to as 'data collection methods in this ACL.

BACKGROUND

The CDSS has the responsibility to protect the personal information and data of IHSS recipients and providers that is stored in CMIPS. As such, CDSS is resolute in enforcing privacy and security provisions regarding the usage of IHSS data, which includes all internal or external data collection methods, counties may utilize to administer their local IHSS program.

As part of the CDSS' responsibility to ensure data security, CDSS will be sending a survey to the counties to identify existing tools and ancillary systems that are being used for data collection. The goal of the survey is to take an inventory of county tools and potentially identify opportunities for possible enhancements to CMIPS reporting that will benefit all counties.

PROHIBITION OF CMIPS DIRECT INTERFACE

The CDSS has developed the CMIPS system and its assorted components with consideration of meeting all counties' IHSS program needs statewide. Counties cannot develop or implement any application, software, etc. that would interface directly with CMIPS due to the potential impact to statewide service for all users. County ancillary systems can utilize the CMIPS data downloads, but any software that uses virtual users, screen scraping, or accesses CMIPS directly is not allowed. Counties shall not develop/procure tools/applications that directly connect to the CMIPS application to perform CRUD (create, read, update and delete) operations to update/maintain IHSS case data.

COUNTY NEW DATA TOOL DEVELOPMENT

With the implementation of this ACL, it is required that counties that would like to implement software that utilizes CMIPS data submit documentation in writing, via email, informing CDSS prior to developing their application.

CDSS will utilize the information from counties to identify and mitigate any risks associated with the use and storage of CMIPS data. Additionally, CDSS will take the opportunity to identify any potential conflicts with planned functionality, where CDSS may be implementing a similar system or enhancement to CMIPS in the future that counties may utilize for the same purpose.

SUBMISSION PROCESS

When transmitting the data tool documentation and any additional system plans and documents to CDSS, the county must include a contact name, telephone number, email address and physical mailing address. This contact information will be used during the review process for clarifying information as needed related to the review process as well as any other communication related to the submission.

The county may submit the data tool documentation consisting of the following information:

- County name
- County contacts: program and technical support
- Name of system or tool
- Vendor developer and contacts (if applicable)
- Proposed implementation date
- Overview of the system/tool: provides high-level description of the system/tool's purpose and function, technical component, data exchange (all inputs and outputs to and from the system/tool), and how the system or tool will be accessed, such as internet or local intranet
- Users: who will use the system/tool
- Description of the county business needs: provide brief description of the business benefits the system/tool will achieve

Counties shall submit their documents to the CMIPSI-Requests@dss.ca.gov email address.

The CDSS will conduct a thorough analysis of the documentation submitted. This process will consist of an examination of how the CMIPS data is going to be used in any new systems or ancillary tools and ensure that there are no potential risks of data breaches of privacy or security.

To complete the analysis, counties, their agents, vendors and/or subcontractors may be required to provide information related to system security, including plans and assessments, and system requirements documentation. Once CDSS completes their analysis, CDSS will notify the requesting county in writing within thirty days if there are any potential issues and provide assistance, if necessary, in resolving and/or mitigating any identified or potential risks associated with the county's plan.

COUNTY RESPONSIBILITIES

Counties are informed that as recipients of State and Federal funding, local county, county agents, vendors and/or sub-contractors may be subject to audit requests from state and/or federal entities, and as such, counties must ensure compliance with such guidelines. Counties must ensure per the Information Practices Act of 1977, Civil Code 1798.3(a) that Personal Identifying Information (PII), and/or Sensitive or otherwise Confidential (PSCI) data is appropriately safeguarded and reclaimed at the completion of agent and/or sub-contractor relationships.

Counties must ensure that their staff and any county agents, vendors and/or sub-contractors may only access IHSS data for purposes of administering the program. Counties may grant public research requests that utilize only aggregate, de-identified data and do not contain PII or PSCI.

To successfully safeguard personal and confidential information, counties must ensure the following items are adhered to:

1. Counties may use the CMIPS Data Download (DDL) files to import any electronic CMIPS data for their reporting needs.
2. Counties, its employees, agents, vendors and subcontractors shall protect from unauthorized disclosure any PSCI.
3. Counties shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PSCI that it creates, receives, maintains, uses, or transmits on behalf of IHSS and CMIPS.
4. Counties shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the county's operations and the appropriate levels of security (confidentiality, integrity, and availability).
5. Counties agree to allow CDSS to inspect systems, ancillary tools and/or records implemented when there is a case of a reported breach of any data from the CMIPS database. Such inspections shall be scheduled at times that take into account the operational and staffing demands at the county.
6. Counties agree to promptly remedy any violation noted as a provision of this ACL.
7. Counties data collection methods must meet both Federal and State laws and regulations that govern technology systems, including but not limited to, the Health Insurance Portability and Accountability Act (HIPAA) and the California Statewide Information Management Manual.

Questions regarding the information transmitted in this ACL may be directed to the Adult Programs Division, CMIPS and Systems Enhancements Branch, at the following email address: CMIPSII-Requests@dss.ca.gov.

Sincerely,

Original Document Signed By:

DEBBI THOMSON
Deputy Director
Adult Programs Division

c: CWDA