

May 4, 2020

CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

EXECUTIVE SUMMARY

**ALL COUNTY WELFARE DIRECTORS LETTER**

This letter provides guidance on existing policy and flexibilities available to county welfare departments relating to income and eligibility verification system (IEVS) processes affected by the statewide outbreak of coronavirus disease 2020 (COVID-19 or novel coronavirus). This ACWDL covers the county welfare departments' need to have IEVS workers process IEVS from home during the stay-at-home order. This ACWDL specifically excludes federal tax information.



**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](http://www.cdss.ca.gov)



**GAVIN NEWSOM**  
GOVERNOR

May 4, 2020

**ALL COUNTY WELFARE DIRECTORS LETTER**

**TO:** ALL COUNTY WELFARE DIRECTORS

**FROM:** NATASHA NICOLAI  
Chief Data Strategist, Deputy Director  
Research, Automation, and Data Division

**SUBJECT:** RECIPIENT INCOME AND ELIGIBILITY VERIFICATION SYSTEM  
PROCESSES DURING COVID-19 EMERGENCY RESPONSE  
EFFORTS

The purpose of this All County Welfare Directors Letter (ACWDL) is to respond to inquiries from county welfare departments (CWDs) related to recipient income and eligibility verification system (R-IEVS) processes during [COVID-19](#). Specifically, this ACWDL covers the requirement for CWD employees to process R-IEVS matches from their homes due to the statewide [stay-at-home order](#) issued March 19, 2020. This ACWDL covers only the time period of the State of California Governor's [Executive Order N-33-20](#), dated March 19, 2020, and later if county or city governments execute similar orders after the end of [N-33-20](#). This guidance only applies for the duration of the [COVID-19](#) situation.

The California Department of Social Services (Department) is working with federal agencies and seeking additional guidance on the expectations of R-IEVS processing during [COVID-19](#). Until the Department receives this federal guidance, the CWDs must continue to meet requirements for remote access to Social Security Administration (SSA) and other personally identifying information (PII) data included in the R-IEVS matches.

This R-IEVS PII data is sourced from the SSA, the California Employment Development Department (EDD), the California Department of Justice (DOJ), and the California Department of Public Health (CDPH).

## **Scope**

Federal tax information (FTI) must **not** be processed remotely and does not come within the scope of this ACWDL.

The R-IEVS matches within the scope of this ACWDL are:

- DPM: Deceased Persons Match
- IFD: Integrated Fraud Detection
- NPM: Nationwide Prisoner Match
- PVS: Payment Verification System
- NHR: New Hire Record
- WIM: Welfare Institutions Match (formerly the California Youth Authority or CYA match)

## **Remote Access Requirements**

In compliance with the SSA, EDD, and Department confidentiality and information security requirements, county partners will use government-issued devices to store and process data. This will ensure that encryption, access control policies, and technological barriers are enforced. In addition, when working from home, employees are required to use a secure virtual private network (VPN) connection, with multifactor authentication (MFA), when accessing government internal networks. Cellular networks must not be used and they must not be used to open a wireless hotspot.

Virtual desktop infrastructure (VDI) managed by the county government IT staff may also be used when employees or contractors are accessing government internal resources using personal equipment. Note that VDIs are only approved for use if the VDI was configured to ensure users cannot copy or move data to their personal devices. The CWDs and employees and contractors must also be aware that the use of personally devices for work-related purposes and materials can bring those devices into scope of federal reviews, audits, or inspections of the use of the data. The CWDs and employees/contractors must be prepared to accept the risks and responsibilities associated with the use of personal devices. See the National Institute of Standards and Technology section below for more information on hardening the security of VPNs, VDIs, and devices.

## **SSA Requirements for Remote Access**

The SSA has provided guidance in their Technical Systems Security Requirements (TSSR, available on request). The most important SSA requirements are listed below:

- Remote connections comply with all applicable federal and state security policy and standards and the access control policy must define the safeguards in place to

adequately protect SSA information for work-at-home, remote access, and/or Internet access (TSSR v8.6, section 5.3).

- Use of both physical and technological barriers to prevent unauthorized retrieval of SSA information via computer, remote terminal, or other means (TSSR v.8.6, section 4.5).
- Operational processes must ensure that no residual SSA information remains on the hard drives of users' workstations after users exit the application(s) that use SSA information (TSSR v8.6, section 5.8).

## **National Institute of Standards and Technology**

All security controls found in the SSA's TSSR as well as other better-known federal safeguard resources originate from the National Institute of Standards and Technology (NIST) special publication (SP) series. The [NIST SP 800](#) series is a comprehensive source of security controls. All R-IEVS data should be evaluated at the Moderate level. The R-IEVS data is PII and as such is confidential.

Relevant [NIST SP 800](#) series documents include, but are not limited to the following:

[NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations](#) is an over-arching safeguards document.

[NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Security](#) covers teleworking and privately-owned devices.

[NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems](#) covers interconnectivity.

## **Physical Protections**

In addition to securing computers, connections, and electronic R-IEVS PII data, the CWD must ensure the physical environment maintains the security and confidentiality of the PII. The following lists the minimum physical requirements for the work-at-home environment:

- Employees and contractors must work in enclosed rooms with no casual visual access, e.g. a person walking past an open window who can view the screen.
- The computer must either remain in the possession of the employee or contractor assigned the device or it must be locked. Physically locking a laptop includes cord locks or placement in a locked cabinet.
- Only county employees or contractors may handle the county-owned computer or device.
- Employees or contractors must not be located outside the United States territories, embassies, or military installations.
- Computer systems that receive, process, store, transmit, or dispose of R-IEVS PII must not be located outside the United States territories, embassies, or military installations.

- Personal devices must not be accessible to other persons within the home during open working sessions.

The Department's Program Integrity Bureau will continue to monitor respective email inboxes for R-IEVS review inquiries, policy interpretation requests, tax intercept inquiries, and special investigation unit inquiries. If you have any questions, please email the Fraud Detection Unit at [FraudDetectionUnit@dss.ca.gov](mailto:FraudDetectionUnit@dss.ca.gov).