

DEPARTMENT OF SOCIAL SERVICES

744 P Street, Sacramento, California 95814



April 6, 1998

ALL-COUNTY INFORMATION NOTICE I-23-98

TO: ALL-COUNTY WELFARE DIRECTORS

Reason For This Transmittal

- State Law Change
- Federal Law or Regulation Change
- Court Order or Settlement Agreement
- Clarification Requested by one or More Counties
- Initiated by CDSS

SUBJECT: SECURITY PROCEDURES FOR ACCESS TO THE CASE MANAGEMENT, INFORMATION, AND PAYROLLING SYSTEM (CMIPS).

REFERENCE: CMIPS USER'S MANUAL, SECTION II-D

The purpose of this All-County Information Notice (ACIN) is to share the results of a recent State Controller's Office (SCO) audit. The audit results indicated a need to remind counties of the security procedures for the Case Management, Information, and Payrolling System (CMIPS) and the CMIPS contractor's data entry documentation needs.

The CMIPS is currently accessed through Electronic Data Systems' (EDS) computer network, EDSNET. The EDSNET network itself is used by EDS employees and customers and contains controls to authorize user access to EDS information systems, thus preventing unauthorized access to sensitive or confidential information. The access to the CMIPS is restricted by requiring the entry of two security codes: a Logon-ID and a password. Logon-IDs are unique six-position alphanumeric codes assigned by EDS to each individual who needs access to the CMIPS. No two users have the same Logon-ID. Passwords are eight-position alphanumeric codes the CMIPS user chooses that verify the accuracy of the Logon-ID.

At any one time, there is only one correct Logon-ID/password combination for each user. The uniqueness of the Logon-IDs, passwords, and their use as a paired combination control the access to the CMIPS. Beyond the Logon-ID and password, access to the CMIPS requires entering specific access codes on a series of screens. In addition, when signing on, the user has three chances to enter the correct Logon-ID/password combination. If the user fails on all three attempts, the Logon-ID is suspended. Also, if a Logon-ID has not been used for a period of 60 days, it is automatically suspended. In order to enable the user to regain their access to the

CMIPS, the CMIPS Security Coordinator at the county must request EDS to reset the Logon-ID and initial password. Passwords expire and must be changed every 30 days; an on-line edit warns the user to change the password prior to its expiration.

Counties are reminded that the security measures for the CMIPS are only effective if there is compliance with the guidelines below. Failure to follow the guidelines and prevent unauthorized access to the information on the CMIPS could result in negative outcomes for both the county and authorized user. With CMIPS access, confidential information may be viewed and used by someone that is not authorized any access. CMIPS access also enables a condition where records and information can be forged or falsified, which could result in incorrect management information and invites fraudulent payments. Also, if a fraudulent action were to occur through an unauthorized access, the tracking of Logon-IDs would indicate that the fraudulent action was made by the authorized user.

In order to prevent unauthorized access and provide security for the information on the CMIPS, the following guidelines are in place:

1. Passwords are to be kept confidential at all times. **Passwords are never written down and never given out or shared with others.** Instead, passwords that are easy to remember but difficult to figure out by another person should be used and kept confidential. Refer to the CMIPS User's Manual, Section II-D-1 for password guidelines.
2. CMIPS access is not to be shared with others. The Logon-IDs are individualized for a specific user's level of access. Only the specified CMIPS user for the Logon-ID and password is authorized to use that access.
3. CMIPS terminals and keyboards are never to be left unattended in a condition that allows unauthorized access after a user has logged-on. In addition, viewing of the information on the CMIPS screens must be restricted to those with authorized access.
4. The county security coordinator function should be centralized with no more than one Security Coordinator per CMIPS site.
5. All requests to add or delete CMIPS users, change access authorization, and resetting Logon-IDs are to be coordinated through the county Security Coordinator.
6. Counties are responsible for compliance with security requirements and must ensure that the central Security Coordinator reviews and does the requested follow-up on any unusual levels of unsuccessful access attempts or potentially unauthorized accesses reported to the county by EDS.

In addition to the on-line CMIPS security issues, the SCO audit indicated a need to remind counties of the importance of following documentation procedures to ensure that only valid timesheet information is entered when the county is unable to access the CMIPS for an extended period of time. In a situation when the county is unable to access CMIPS, and EDS is requested to assist the county with their data entry needs, the only method to ensure that accurate and valid information is entered on the CMIPS, is by having the county submit all of the supporting documentation for the EDS data entry work. The documentation instructions are in the CMIPS Manual Section VII-G. The county will be responsible to ensure the timely delivery of the supporting documentation.

Please contact either your EDS Business Analyst or Craig Tanaka at (916) 229-4017 regarding your questions on this ACIN.

Sincerely,



DONNA L. MANDELSTAM
Deputy Director
Disability and Adult Programs Division