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

CDSS
WILL LIGHTBOURNE
DIRECTOR

EDMUND G. BROWN JR.
GOVERNOR

January 9, 2015

ALL-COUNTY LETTER NO.: 15-05

REASON FOR THIS TRANSMITTAL

[ ] State Law Change
[ ] Federal Law or Regulation Change
[ ] Court Order
[ ] Clarification Requested by One or More Counties
[X] Initiated by CDSS

TO: ALL COUNTY WELFARE DIRECTORS
ALL ADULT PROTECTIVE SERVICES (APS) PROGRAM MANAGERS

SUBJECT: SELF-CERTIFICATION TRAINING FOR ALTERED ACCESS TO MEDI-CAL ELIGIBILITY DATA SYSTEM (MEDS) DATA ELEMENTS

REFERENCE: ALL COUNTY LETTER (ACL) 12-31, DATED JUNE 28, 2012

The purpose of this letter is to inform county Adult Protective Services (APS) program staff of the availability of MEDSLite data and to instruct counties on the implementation of the self-directed certification training document, Training for the Access and Use of Electronically Exchanged Data Provided by the Social Security Administration (SSA), (see attached) for the access and use of electronically exchanged data based on the strict security and privacy requirements provided by the SSA.

BACKGROUND

Access to the SSA data, which is maintained in the Medi-Cal Eligibility Data System (MEDS), requires strict security and privacy requirements. To be in full compliance with SSA requirements, the California Department of Social Services (CDSS) released ACL No. 12-31, on June 28, 2012, which provided information to all County Welfare Directors and all County APS program managers regarding changes in access to the MEDS data elements for APS case work. Because APS program requirements do not require federal or state eligibility or a means test for APS services, APS program staff should not have access to the MEDS data. ACL No. 12-31 specified that effective June 30, 2012, county APS program staff shall not access the MEDS data for the purpose of APS case work. However, counties may continue to access the MEDS data for In-Home Supportive Services (IHSS) case work.

An Interagency Agreement has been executed between CDSS and the Department of Health Care Services (DHCS) to procure data access for county APS program staff through the MEDSLite database, a subset of the MEDS database that meets compliance with the privacy and security requirements of the SSA. DHCS is currently in contact with counties to identify APS program staff that will have access to the MEDSLite database.

TRAINING REQUIREMENT

The purpose of this self-directed training is to ensure full compliance with the SSA strict adherence to security and privacy requirements regarding accessibility of the authorized and unauthorized uses of the confidential information in the MEDS data by all county APS program staff. The self-directed training shall be implemented immediately upon release of this ACL.

This self-directed training requires that all county APS program staff read and understand the training document. Sections 1, 2 and 3 of the training document clarify the authorized vs unauthorized use of the MEDS data. The self-directed training also includes an "Interactive Question and Answer Section," to be completed by county APS program staff. By signing the training document, the county APS program staff acknowledges that they have reviewed Sections 1, 2 and 3 of the document and completed the "Interactive Question and Answer Section," and that they understand the authorized vs unauthorized use of the MEDS data. The self-directed training is for the lawful use of SSA data by county APS program staff.

All APS supervisors and managers should review each completed self-directed training document to verify that the employee has self-corrected any missed or incorrect answers, and to ensure full compliance with the SSA requirements. All APS supervisors and managers shall maintain the original signed self-directed training documents as required by the SSA for auditing purposes.

If you have questions or comments regarding this ACL, please contact Adult Programs Policy and Quality Assurance Branch, Policy and Operations Bureau, Provider Policy and Adult Protective Services Unit at (916) 651-5350.

Sincerely,

Original Document Signed By:

EILEEN CARROLL
Deputy Director
Adult Programs Division

Attachment

c: CWDA

ATTACHMENT

Training for the Access and Use of Electronically Exchanged Data Provided by the SSA

The purpose of this training is to inform you of authorized and unauthorized uses of the Medi-Cal Eligibility Data System (MEDS) based on the confidential information in MEDS provided by the federal Social Security Administration (SSA). You are required to review Sections 1, 2 and 3 below, complete the Interactive Question and Answer section, and sign and date this form verifying that you understand the authorized and unauthorized use of MEDS.

Section 1 - Authorized and Unauthorized Use of MEDS

- The SSA provides electronically exchanged confidential data to the State of California that is incorporated into MEDS.
- The use of the SSA data is pursuant to a federal computer matching data agreement that strictly limits the use of the data provided by the SSA.
- The data provided by the SSA for MEDS includes personally identifiable information.
- The Information Exchange Agreement between the State of California and the SSA is required pursuant to the Computer Matching and Privacy Protection Act (CMPPA) of 1988, and the Computer Matching and Privacy Protection Amendments of 1990, enacted by Congress to protect an individual's privacy rights from the indiscriminate use of computer records.
- The SSA recently determined that the accessing and use of MEDS containing SSA data for the Adult Protective Services (APS) program violated the CMPPA and is required to be discontinued.
- The California Department of Social Services (CDSS) issued an All County Letter (ACL NO. 12-31) to the counties to cease access and use of MEDS for the APS program.
- <u>County employees performing services for the APS program are not authorized to access or use MEDS.</u>
- Unauthorized access and use of MEDS is a violation of the CMPPA and may be in violation of other state and federal privacy laws.
- The In-Home Supportive Services (IHSS) program is part of the federal Medicaid program under Title XIX of the Social Security Act, which the SSA has approved the use of the SSA records for program purposes.
- A county worker who provides services for IHSS may be authorized to access and use MEDS.
- A county worker who provides services for APS is prohibited from accessing and using MEDS. A county worker who provides services for both IHSS and APS is prohibited from accessing and using MEDS under the premise of providing services for IHSS but using the information for APS.
- Unauthorized access and use of MEDS for APS program purposes is identifiable and will be actively monitored by CDSS and the Department of Health Care Services (DHCS).

- Unauthorized use of MEDS may subject the violator to state and federal civil and criminal penalties.

Section 2 - Required Protections of Personally Identifiable Information (PII)

- Personally identifiable information provided by the SSA includes names, Social Security Numbers, addresses, amounts and other information related to SSA benefits and earnings information.
- Use and access to PII in a computerized system or other form of records is restricted to authorized users with a need to know.
- An authorized user is responsible for safeguarding the PII from inadvertent disclosure, loss or theft.
- Encryption of all computer laptops or media storage devices regardless of locations of use is required if it contains PII.
- Encryption of emails is required if the email contains PII and must meet acceptable standards designated by the National Institute of Standards and Technology.
- Standards of encryption acceptable to the SSA for transmitting data over the internet are Advanced Encryption Standard (AES) or triple Data Encryption Standards (DES3) if AES is unavailable.

Definitions:

1. Provided by the SSA:
    - **Breach:** Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII, whether physical, electronic, or in spoken work or recording.
    - **Security Breach**: An act from outside an organization that bypasses or contravenes security policies, practices, or procedures.
    - **Security Incident:** A fact or event which signifies the possibility that a breach of security may be taking place, or may have taken place.
    - **Security Violation:** An act from within an organization that bypasses or contravenes security policies, practices, or procedures.
    - *Note: These definitions were obtained from the Electronic Information Exchange Agreement Security Requirements and Procedures for State and Local Agencies Exchange Information with the SSA, p. 22 and 24, Ver. 6.0, April 23, 2012.*

2. Provided by Other Sources:
    - Types of techniques:
        - **Phishing:** When attackers use social engineering techniques to trick users into accessing a fake Web site and divulging personal information. In some phishing attacks, attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site. (NIST SP 800-44)

- **Pharming:** When attackers use technical means, instead of social engineering, to redirect users into accessing a fake Web site masquerading as a legitimate one and divulging personal information. (NIST SP 800-44)
- **Spoofing:** When attackers fake the sending address of a transmission to gain illegal [unauthorized] entry into a secure system. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. (CNSSI 4009)

- Types of tools:
  - **Malware or Malicious Code:** Software that compromises the operation of a system by performing an unauthorized function or process. (NIST SP 800-53)
  - **Spyware:** Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner. (NIST SP 800-53)
  - **Trojan horse:** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI 4009)

Breach Notification

A user of MEDS is required to immediately notify his/her supervisor of a suspected or actual breach of security or unauthorized disclosure of PII to facilitate an investigation and required that a breach has occurred. For the SSA PII made available through MEDS, the initial notification to DHCS must be made (within 1 hour of experiencing or suspecting a breach or loss of PII). A user of MEDS, may also directly and immediately report the suspected or actual breach of security or unauthorized disclosure of PII, as follows:

Manuel Urbina
Chief, Security Unit Policy Operations Branch
Medical Operations Branch
1501 Capitol Avenue, MS 4607
Sacramento, CA 95814
(916) 650-0160
Email: Manual.Urbina@dhcs.ca.gov

If he is unavailable, the breach must be reported to each of the following:

SSA Point of Contact:
Dolores Dunnachie, Director
Center for Programs Support
San Francisco Regional Office
1221 Nevin Avenue
Richmond, CA 94801
Phone: (510) 970-8444
Fax: (510) 970-8101
Dolores.Dunnachie@ssa.gov
SSA--Security Issues Contact:

Michael G. Johnson, Acting Director
Office of Information Exchange
Office of Electronic Strategic Services
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0266
Fax: (410) 966-0527
Email: Michael.G.Johnson@ssa.gov

If none of the above are available the breach must be reported to the SSA National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list).

Section 3 - Requirements of Protecting Confidential Information

Individuals authorized to access and use confidential data for employment purposes are required to protect and maintain confidentiality data of applicants and recipients applying for and receiving public assistance or social services. (Welfare & Institutions Code Section 10850 and the CDSS Manual of Policies and Procedures, Division 19, Confidentiality, Fraud, Civil Rights and State Hearings

Interactive Question and Answer Section

Please answer true or false by circling the T or F in items 1-13. Please circle the letter with the most appropriate response:

1. The SSA and the State of California must execute a federal computer data matching agreement for the SSA to provide data to the State of California. (T) / (F)
2. The use of the SSA data by the counties is authorized by the federal computer matching data agreement that strictly limits the use of the data provided by the SSA. (T) / (F)
3. The requirement for a Computer Data Matching and Privacy Agreement between the State of California and the SSA is through an executive order of the president. (T) / (F)
4. Unauthorized disclosure of SSA data is prohibited by federal law. (T) / (F)
5. Data provided by the SSA is incorporated into MEDS. (T) / (F)
6. DHCS has the ability to identify and track MEDS users and the data accessed by the user at the county level. (T) / (F)
7. A county employee may not access or use MEDS in providing Adult Protective Services (APS). (T) / (F)
8. A county employee may access or use MEDS in providing In-Home Supportive Services (IHSS). (T) / (F)
9. A county employee who is authorized to access and use MEDS for IHSS program purposes may also use the information obtained for APS purposes. (T) / (F)
10. Unauthorized access and use of MEDS may violate federal and state laws and result in civil and criminal penalties. (T) / (F)
11. Only verified data breaches of PII must be reported to the SSA. (T) / (F)
12. Only a supervisor is allowed to report a data breach of the PII in MEDS to the SSA. (T) / (F)
13. Phishing attackers use social engineering techniques to trick users into accessing a fake Web site and divulging personal information. (T) / (F)
14. I will not access or disclose confidential information in MEDS to provide APS because:
    a. The SSA has determined its use is not permitted under the CMPPA.
    b. It may be determined that I violated federal and state laws resulting in civil and criminal penalties.
    c. DHCS is capable of tracking users and accessed data to determine unauthorized use of MEDS.
    d. All of the Above.

Certification of Completion

I _____ (print name), by signing this document acknowledge that I have reviewed and understand Sections 1, 2 and 3 and completed the Interactive Question and Answer section. I understand that accessing and use of MEDS data in providing adult protective services is prohibited by law and that the unauthorized use of MEDS may result in violations of state and/or federal laws with civil and/or criminal penalties. I acknowledge that I have provided my supervisor with the original signed copy of this document and I have retained a copy for my records.

County of: _____ Signature: _____
Department/Division: _____ Date: _____

Review and Message to Supervisor

This training is for the lawful use of SSA data by county workers and should be a tool that is easily referred to by the employee, when necessary. All supervisors should review all completed training to verify that the employee has self-corrected any missed or incorrect answers.

Answers to the Training

1. T
2. T
3. F
4. T
5. T
6. T
7. T
8. T
9. F
10. T
11. F
12. F
13. T
14. (D) All of the above

For questions or comments regarding the use of this training tool please contact:

Information Security Office
California Department of Social Services
744 P Street
Sacramento CA, 95814
Email address: iso@dss.ca.gov