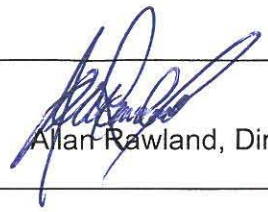
County of San Bernardino
Department of Behavioral Health

Medi-Cal Eligibility Data Systems (MEDS) Policy

Effective Date 06/30/2010
Approval Date 10/04/2010



Allan Rawland, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to adhere to privacy and security requirements that are in accordance with the Medi-Cal Privacy and Security Agreement between the California Department of Mental Health (DMH) and the County of San Bernardino Department of Behavioral Health (DBH) regarding the Medi-Cal Eligibility Data System (MEDS).

Purpose

Provide DBH staff with the requirements of MEDS, specifically, the following:

- General use of the system,
- Security and privacy safeguards,
- Unacceptable use and
- Enforcement policies associated.

Important Note: As DBH is a covered entity bound to adhere to state and federal confidentiality and privacy laws, staff are required to apply those laws and regulations which provide the greatest degree of protection and autonomy for its clients.

Definitions

Department of Health Care Services (DHCS): State department responsible for the administration of the Medi-Cal program and who delegates the administration of the Specialty Mental Health Services program to DMH.

Medi-Cal PII: Personally identifiable information (PII) obtained from the federal Social Security Administration (SSA) via MEDS that can be used, alone or in conjunction with any other information, to identify a specific individual or can be used to search for or identify individuals or can be used to access an individual's file. Examples of Medi-Cal PII include the following: name, social security number, Social Security benefit data, date of birth, official State or government issued driver's license or identification number.

MEDS: Medi-Cal Eligibility Data System that contains data from SSA that is related to Social Security beneficiaries, Supplemental Security Income beneficiaries, beneficiaries' eligibility for Medi-Cal, certain veterans' benefits, and certain tax return information.

MEDS Agreement: Medi-Cal Privacy and Security Agreement between DMH and DBH detailing privacy and security requirements of personally identifiable information of Medi-Cal beneficiaries accessed via MEDS.

Continued on next page

Definitions (continued)

MEDS Coordinator: designated person within DBH that is the primary point of contact for DHCS regarding MEDS who is responsible for MEDS access i.e., determining staff eligibility, providing and terminating, etc.

MEDS Liaison: designated person within DBH that is the primary point of contact for staff when requesting password resets.

Terms of the MEDS Agreement

Per the terms of the MEDS Agreement, DBH is required to complete the following:

- Train staff having authorized access;
- Establish and maintain oversight and monitoring for staff having authorized access;
- Obtain confidentiality statements from staff having authorized access;
- Ensure physical security of Medi-Cal PII;
- Comply with computer security safeguards of Medi-Cal PII;
- Implement and maintain paper document controls regarding Medi-Cal PII;
- Notify and investigate breaches of Medi-Cal PII; and
- Comply with the MEDS Agreement.

Access Limitations for DBH and General Use

The MEDS Agreement limits authorization to those employees of the Medi-Cal Specialty Mental Health Services that assist in the administration of the Medi-Cal Program by determination of eligibility for mental health services.

DBH staff having authorized access to MEDS may use or disclose Medi-Cal PII only to perform functions, activities or services directly related to the determination of eligibility for mental health services.

DBH has determined only applicable staff from the following programs are authorized and eligible for MEDS access:

- Access Unit
- Benefits Team
- Community Crisis Response Teams
- Crisis Walk-In Clinics
- Diversion
- Financial Interviewers
- Information Technology
- Quality Management
- Business Office

Continued on next page

Security and Privacy Safeguards

While it is the responsibility of the Department to ensure the following safeguards are in place to protect the security and privacy of MEDS PII:

- Physical Security;
- Computer Security;
- System Security;
- Audit Controls; and
- Paper Document Controls

DBH staff having authorized access to MEDS are responsible to safeguard Medi-Cal PII from loss, theft or inadvertent disclosure with the following security and privacy safeguards, including but not limited to the following:

- Accessing and using MEDS to perform official job duties as they associate to the determination of eligibility for mental health services;
- Adhering to County and DBH Dress Code by wearing identification badge to identify themselves as DBH employee;
- Maintaining the confidentiality of the MEDS login information;
- Creating and utilizing a password in accordance with DBH Policy IT5009, User I.D. and Password Policy;
- Using one's own MEDS login and password to access MEDS,
- Maintaining possession of Medi-Cal PII on DBH grounds;
- Securing and storing all Medi-Cal PII in locked file cabinets, rooms or desks when not in use;
- Securing printed Medi-Cal PII from inappropriate access, not leaving on printers, fax machines or copiers;
- Maintaining possession of Medi-Cal PII when transporting in a vehicle or airplane;
- Preventing unauthorized users or visitors the ability to access, control or view Medi-Cal PII accessed via MEDS;
- Locking the computer if MEDS screens are up to prevent access or view of Medi-Cal PII;
- Disposing of Medi-Cal PII properly in locked shred containers;
- Adhering to DBH Policy COM0901, Sending Confidential Information by Facsimile Policy when sending faxes;
- Adhering to DBH Policy IT0909, Electronic Transfer of Client Protected Health Information – Internet and Intranet Policy, regarding the sending of electronic mails;
- Adhering to DBH Policy IT5008, Device and Media Controls Policy regarding the use of communication devices with proper control mechanisms and approvals; and
- Reporting any anomalies, breaches, disclosures or acquisition of Medi-Cal PII to the DBH Office of Compliance immediately the same day as when identified as occurred or to have possibly occurred.

Continued on next page

Prohibited Use and Activities

DBH staff having authorized access are prohibited from the following activities regarding MEDS and/or MEDS PII, including but not limited to the following:

- Sharing password or login information;
- Making password or login information accessible to unauthorized persons;
- Providing MEDS information or printouts to unauthorized persons, including but not limited to:
  - other County departments and
  - contract agencies.
- Removing MEDS screen prints from DBH grounds;
- Failing to properly secure and store Medi-Cal PII in a locked cabinet;
- Leaving workstation monitor unlocked when unattended;
- Storing Medi-Cal PII in a vehicle;
- Permitting Medi-Cal to be checked in as luggage for an airline flight or other modes of public transportation;
- Allowing access, use or view Medi-Cal PII to unauthorized persons;
- Failing to adhere to DBH policies regarding the use of fax machines, electronic mail and/or other communication devices relating to Medi-Cal PII; and
- Accessing MEDS for purposes other than to perform official job duties related to the determination of eligibility for mental health services.

MEDS Screen Limitations

Mental Health Plans (MHPs) providing Medi-Cal Specialty Mental Health Services are authorized to receive limited data from MEDS, including but not limited to data from the following screens:

- SDX: State Data Exchange
- BENDEX: Beneficiary and Earnings Data Exchange Systems
- SVES: State Verification and Exchange System
- EVS: Enumeration Verification System

MEDS Access and Contacts

DBH staff may refer to the MEDS Access and Contacts Procedure for requesting authorized access to MEDS and to obtain information of the roles and responsibilities for MEDS Contacts.

Enforcement Policies

In order to meet the privacy and security requirements of the MEDS Agreement, DBH shall adhere to this policy as well as the County and DBH policies listed in the Related Policies and Procedures section of this policy.

Continued on next page

Violations

Authorized DBH staff having access to MEDS who access, disclose or use Medi-Cal PII in a manner or for a purpose not related to the determination of eligibility for mental health services may be subject to loss of MEDS access, disciplinary action up to and including termination and/or civil or criminal liability.

References

CA Civil Code, Section 56 et al., California Confidentiality of Medical Information Act
Medi-Cal Privacy and Security Agreement
Social Security Act, Sections 1137 and 453
Title 45 of the Code of Federal Regulations, Section 164 et al., Health Insurance Accountability and Portability Act of 1996
Welfare and Institutions Code, Section 14100.2

Related Policies and Procedures

County of San Bernardino Policy Manual, 16-01, Non-Public Personally Identifiable Information
County of San Bernardino Policy Manual, 16-02, Protection of Individually Identifiable Health Information
County of San Bernardino Standard Practice, 16-02SP1, Protection of Individually Identifiable Health Information
DBH Standard Practice Manual, COM0901, Sending Confidential Information by Facsimile Policy
DBH Standard Practice Manual, COM0905, Client Privacy and Confidentiality of Protected Health Information
DBH Standard Practice Manual, COM0907, Unauthorized Access of Confidential Medical Records Policy
DBH Standard Practice Manual, COM0909, Electronic Transfer of Client Protected Health Information – Internet and Intranet Policy
DBH Standard Practice Manual, COM0924, Workstation and System Security Policy
DBH Standard Practice Manual, COM0925, Data Integrity Policy
DBH Standard Practice Manual, COM0926, HIPAA Violation Sanctions Policy
DBH Standard Practice Manual, COM0943-1, MEDS Access and Contacts Procedure
DBH Standard Practice Manual, COM0944, Privacy or Security Breach Policy
DBH Standard Practice Manual, IT5004, Computer and Network Appropriate Use Policy
DBH Standard Practice Manual, IT5005, Electronic Mail Policy
DBH Standard Practice Manual, IT5006, Remote Access Policy
DBH Standard Practice Manual, IT5008, Device and Media Controls Policy
DBH Standard Practice Manual, IT5009, User I.D. and Password Policy