

MEDI-CAL PRIVACY AND SECURITY AGREEMENT BETWEEN The California Department of Mental Health and the County of Napa, Department of Health and Human Services

PREAMBLE

The California Department of Mental Health (DMH) and the County of Napa, Department of Health and Human Services ("County Department") enter into this Medi-Cal Data Privacy and Security Agreement ("Agreement") in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII).

The Department of Health Care Services (DHCS) receives federal funding to administer the Medi-Cal program. DHCS delegates the administration of the Specialty Mental Health Services to DMH. DMH contracts with County Health Plans (MHPs) for the provision of Specialty Mental Health Services.

This Agreement covers the County of <u>Napa</u>, Department of <u>Health and Human Services</u> workers that assist in the administration of the Medi-Cal program; and access, use, or disclose Medi-Cal PII. For the purpose of this agreement, the following terms mean:

- 1. "Assist in the Administration of the Medi-Cal Program" is performing an administrative function on behalf of Medi-Cal, such as determining eligibility or case managing IHSS (In-Home Supportive Services) clients and;
- 2. "Medi-Cal PII" is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal, such as determining Medi-Cal eligibility or conducting IHSS operations, that can be used alone, or in conjunction with any other information, to identify a specific individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper.

AGREEMENTS

NOW THEREFORE, DMH and the County Department mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

- A. County Department workers covered by this Agreement ("County Workers") may use or disclose Medi-Cal PII only to perform functions, activities or services directly related to the administration of the Medi-Cal program in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq, or as required by law. For example, County Workers performing eligibility determinations may generally only use or disclose Medi-Cal PII to determine eligibility for individuals apply for Medi-Cal. County Workers assisting in the administration of the In-Home Supportive Services (IHSS) program may generally use or disclose Medi-Cal PII only to perform administrative functions essential to the operation of the IHSS program. Disclosures which are required by law, such as court order, or which are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.
- B. Access to Medi-Cal PII shall be restricted to only <u>County Workers</u> who need the Medi-Cal PII to perform their official duties in connections with the administration of the Medi-Cal program.
- C. County Workers who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PRIVACY AND CONFIDENTIALITY

The County Department agrees to advise County Workers who have access to Medi-Cal PII of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department shall:

A. Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII; and take corrective action against such County Worker who intentionally violates any provisions of this Agreement, up to and including by termination of employment. In complying with this agreement, the County Department agrees to:

- B. Provide privacy and security awareness training to each new County Worker within 30 days of employment and thereafter provide ongoing reminders of the privacy and security safeguards in this Agreement to all County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII.
- C. Maintain records indicating each County Worker's name and the date on which the initial privacy and security awareness training was completed.
- D. Retain training records for inspection for a period of three years after completion of the training.

III. MANAGEMENT OVERSIGHT AND MONITORING

The County Department agrees to:

- A. Establish and maintain ongoing management oversight and quality assurance for monitoring workforce compliance with the privacy and security safeguards in this Agreement when using or disclosing Medi-Cal PII.
- B. Ensure that ongoing management oversight includes periodic self-assessments and randomly sampling work activity by County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII. DHCS/DMH shall provide the County with information on MEDS usage indicating any anomalies for investigation and follow-up.
- C. Ensure that these management oversight and monitoring activities are performed by County Workers whose job functions are separate from those who use or disclose Medi-Cal PII as part of their routine duties.

IV. CONFIDENTIALITY STATEMENT

The County Department agrees to ensure that all County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by County Worker prior to access to Medi-Cal PII.

V. PHYSICAL SECURITY

The County Department shall ensure Medi-Cal PII is used and stored in an area that is physically safe from access by authorized persons during working hours and non-working hours. The County Department agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure, and therefore, agrees to:

- A. Secure all areas of County Department facilities where County Workers assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII. The County Department shall ensure that these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or access authorization; and access to premises is by official identification.
- B. Ensure that there are security guards or a monitored alarm system with or without security cameras 24 hours a day, 7 days a week at County Department facilities and leased facilities where a large volume of Medi-Cal PII is stored.
- C. Issue County Workers who assist in the administration of the Medi-Cal program identification badges and require County Workers to wear these badges at County Department facilities where Medi-Cal PII is stored or used.
- D. Store paper records with Medi-Cal PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks or locked offices in facilities where are multi-use, meaning that there are County Departments and non-County Department functions in one building in work areas that are not securely segregated from each other. The County Department shall have policies that indicate County Workers are not to leave records with Medi-Cal PII unattended at any time in vehicles or airplanes and not to check such records in baggage on commercial airplanes.
- E. Use all reasonable measure to prevent non-authorized personnel and visitors from having access to, control of, or viewing Medi-Cal PII.

VI. COMPUTER SECURITY SAFEGUARDS

The County Department agrees to comply with the general computer security safeguards, system security controls, and audit controls in this section.

General Computer Security Safeguards

In order to comply with the following general computer security safeguards, the County Department agrees to:

- A. Encrypt portable computer devices, such as laptops and notebook computers that process and/or store Medi-Cal PII, with a solution using a vendor product that has been validated by the National Institute of Standards and Technology (NIST) as meeting Federal Information Processing Standard (FIPS) Publication 140-2 requirements, and is recognized as the industry leader in meeting the needs of the intended solution. The County Department shall use an encryption solution that is full-disk unless otherwise approved by DHCS.
- B. Encrypt workstations where Medi-Cal PII is stored using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution.
- C. Ensure that only the minimum necessary amount of Medi-Cal PII is downloaded to a laptop or hard drive when absolutely necessary for current business purposes.
- D. Encrypt all electronic files that contain Medi-Cal PII when the file is stored on any removable media type devise (i.e. USB thumb drives, floppies, CD/DVD. Etc.) using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution.
- E. Ensure that all emails sent outside the County Department's e-mail environment that include Medi-Cal PII are sent via an encrypted method using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution.
- F. Ensure that all workstations, laptops and other systems that process and/or store Medi-Cal PII have a commercial third-party anti-virus software solution and are updated when a new anti-virus definition/software release is available.
- G. Ensure that all workstations, laptops and other systems that process and/or store Medi-Cal PII have current security patches applied and up-to-date.

- H. Ensure that all Medi-Cal PII is wiped from systems when the data is no longer legally required. The County Department shall ensure that the wipe method conforms to Department of Defense standards for data destruction.
- I. Ensure that any remote access to Medi-Cal PII is established over an encrypted session protocol using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution. The County Department shall ensure that all remote access is limited to minimum necessary and least privilege principles.

System Security Controls

In order to comply with the following system security controls, the County Department agrees to:

- J. Ensure that all County Department systems containing Medi-Cal PII provide an automatic timeout after no more than 20 minutes of inactivity.
- K. Ensure that all County Department systems containing Medi-Cal PII display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User shall be directed to log off the system if they do not agree with these requirements.
- L. Ensure that all County Department systems containing Medi-Cal PII log successes and failures of user authentication and authorizations granted. The system shall log data changes and system accesses conducted by all users (including all levels of users, system administrators, developers, and auditors). The system shall have the capability to record data access for specified users when requested by authorized management personnel. A log of all system changes shall be maintained and be available for review by authorized management personnel.
- M. Ensure that all County Department systems containing Medi-Cal PII use role based access controls for all user authentication, enforcing the principle of least privilege.
- N. Ensure that all County Department data transmissions over networks outside of the County's controls are encrypted end-to-end using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution, when transmitting Medi-Cal PII. The County Department shall encrypt Medi-Cal PII at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable.

O. Ensure that all County Department systems that are accessible via the Internet or store Medi-Cal PII activity use either a comprehensive third-party real-time host based intrusion detection and prevention program or be protected at the perimeter by a network based IDS/IPS solution.

Audit Controls

In order to comply with the following audit controls, the County Department agrees to:

- P. Ensure that all County Department systems processing and/or storing Medi-Cal PII have at least an annual system security review. The County Department review shall include administrative and technical vulnerability assessments.
- Q. Ensure that all County Department systems processing and/or storing Medi-Cal PII have an automated audit trail, which includes the initiator of the request, along with a time and date stamp for each access. These logs shall be read-only and maintained for a period of at least three (3) years. There shall be a routine procedure in place to review system logs for unauthorized access. The County Department shall investigate anomalies identified by interviewing County Workers and witnesses and taking corrective action, including by disciplining County Workers, when necessary.
- R. Maintain an automated audit trail record identifying either the individual worker or the system process that initiated a request for information from Social Security Administration (SSA) for its systems, such as IEVS. Individual audit trail records shall contain the data needed to associate each query transaction to its initiator and relevant business purpose (that is, the client record for which SSA data was accessed) and each transaction shall be time and date stamped. Access to audit file shall be restricted to authorized users with a need to know and the audit file data shall be unalterable (read only) and maintained for a minimum of three years.
- S. Investigate anomalies in MEDS usage identified by DHCS and report conclusions of such investigations and remediation to DHCS.
- T. Exercise management control and oversight, in conjunction with DHCS/DMH, of the function of authorizing individual user access to SSA data and MEDS and over the process of issuing and maintaining access control numbers and passwords.

U. Ensure that all County Department systems processing and/or storing Medi-Cal PII have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

VII. PAPER DOCUMENT CONTROLS

In order to comply with the following paper document controls, the County Department agrees to:

- A. Dispose of Medi-Cal PII in paper form through confidential means, such as cross cut shredding and pulverizing.
- B. Not remove Medi-Cal PII from the premises of the County Department except for identified routine business purposes or with express written permission from DHCS.
- C. No leave faxes containing Medi-Cal PII unattended and keep fax machines in secure areas. The County Department shall ensure that faxes contain a confidentiality statement notifying persons receiving faxes in error to destroy them. County Workers shall verify fax numbers with the intended recipient before sending.
- D. Use a secure, bonded courier with signature of receipt when sending large volumes of Medi-Cal PII. The County Department shall ensure that disks and other transportable media sent through the mail are encrypted using a vendor product validated by NIST as FIPS 140-2 compliant, and is recognized as an industry leader in meeting the needs of the intended solution.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES

The County Department agrees to:

A. Notify DMH/DHCS immediately by telephone call or —mail upon the discovery of a breach of security of Medi-Cal PII in computerized form if the PII was, or is reasonably believed to have been, acquired by an unauthorized person; or within 24 hours by telephone call or e-mail of the discovery of any other suspected security incident, intrusion, loss or unauthorized use or disclosure of PII in violation of this Agreement or the law. The County Department shall submit the notification to the DHCS Privacy Officer and the DHCS and DMH Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PII, the County Department shall notify DHCS by calling the DHCS ITSD Help Desk.

DHCS Privacy Officer	DHCS Information Security Officer
Privacy Officer c/o: Office of Legal Services Department of Health Care Services P.O Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone:	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899- 7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 (800)
(916) 445-4646	DMH Information Security Officer Aaron Jones Information Security Officer 1600 Ninth Street, Room 433 Sacramento, CA 95814 Email: iso@dmh.ca.gov
	Telephone: (916) 651-6776

- B. Ensure that the initial notification includes contact and component information; a description of the breach or loss with scope, number of files or records, type of equipment or media, approximate time and location of breach of loss; description of how the data was physically stored, contained, or packaged (e.g. password protected, encrypted, locked briefcase, etc.); whether any individuals or external organization have been contacted; and whether any other reports have been filed.
- C. Take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment.
- D. Investigate the breach and produce a written breach report within ten working days of the incident, containing details of the incident; date the incident occurred; date the incident was detected; location of the incident; media/device type, if applicable; if the media was encrypted, if applicable; costs associated with the incident; number of individuals affected; a detailed corrective action plan including measures that were taken to halt and/or contain the breach; estimated cost of corrective actions; and the date corrective actions will be fully implemented. The County Department shall submit the breach report to the DHCS Privacy Officer and DHCS and DMH Information Security Officers.

E. Notify individuals of the breach or unauthorized use or disclosure of Medi-Cal PII maintained by the County Department when notification is required under state or federal law. The County Department shall obtain the approval of the DHCS Privacy Officer for the time, manner and content of any such required notifications. County Department shall be responsible for the cost of such notification to the extent that such breach or unauthorized use or disclosure is due to the negligence or intentional misconduct of County Department. To the extent such breach or unauthorized use or disclosure is due to the negligence or intentional misconduct of DHCS, DHCS shall be responsible for notifying individuals and the County Department shall not be responsible for any costs of notification. If there is any question as to whether DHCS or the County Department is responsible for the breach, DHCS shall issue the notice and DHCS and the County Department shall subsequently determine responsibility for purposes of allocating the costs of such notices.

IX. COMPLIANCE WITH SSA AGREEMENT

The County Department agrees to comply with substantive privacy and security requirements in the Agreement between Social Security Administration and DMH, known as the 1137 Agreement, which is appended t and hereby incorporated into this Agreement (Exhibit A). The specific sections of the 1137 Agreement which contain substantive privacy and security requirements which are to be complied with by County Department are as follows: XI. Procedures for Security; XII. Safeguarding and Report Responsibilities for Personally Identifiable Information (PII); XIII. Procedures for Records Usage, Duplication, and Redisclosure Restrictions; and Attachment C, Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from Social Security Administration. If there is any conflict between a privacy and security standard in these sections of the 1137 Agreement and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means that standard which provides the greatest protection to data.

X. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the County Department agrees to allow DHCS and/or DMH to inspect the facilities, systems, books and records of the County Department, with reasonable notice from DHCS/DMH, in order to perform assessments and review. Such inspections shall be scheduled at times that take into account the operational and staffing demands of the county. The County Department agrees to promptly remedy any violation of any provision of this Agreement and certify the same to the DHCS Privacy Officer and DHCS/DMH Information Security Officer in writing, or to enter into a written corrective action plan with DHCS/DMH containing deadlines for achieving compliance with specific provisions of this Agreement.

XI. DEADLINE FOR SUBSTANTIAL COMPLIANCE

- A. The County Department shall be in substantial compliance with this Agreement by no later than July 1, 2010.
- B. If, at any time, the county is unable to meet the security and privacy requirements imposed in this Agreement in the manner specified therein due to a lack of funding;
 - a. DHCS/DMH will work with the county to develop a Corrective Action Plan which can be implemented within the resources provided by the state for this purpose and which is intended to substantially meet those security and privacy requirements even if such requirements are met utilizing alternative or different methods than those specified in this Agreement.
- C. DHCS and/or DMH shall monitor corrective action plans which County Department develops to remediate gaps in security compliance under this Agreement and reassess compliance.

XII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

In the event of litigation or administrative proceedings involving DHCS/DMH based upon claimed violations by the County Department of the privacy or security of Medi-Cal PII, or federal or state laws or agreements concerning privacy or security of Medi-Cal PII, the County Department shall make all reasonable effort to make itself and County Workers assisting in the administration of the Medi-Cal program and using or disclosing Medi-Cal PII available to DHCS/DMH at no cost of DHCS/DMH to testify as witnesses. DHCS/DMH shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to County Department at no cost to County Department to testify as witnesses, in the event of litigation or administrative proceedings involving the County Department based upon claimed violations by DHCS of the privacy or security of Medi-Cal PII, or state or federal laws or agreements concerning privacy or security of Medi-Cal PII.

XIII. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement.

Medi-Cal Privacy and Security Agreement County of <u>Napa</u>

The authorized officials whose signatures a respective agencies to the terms of this Agr 2009.	ppear below have committed their July, eement effective this Day of July,
For the County of <u>Napa</u> , Department of <u>Hea</u>	lth and Human Services:
Alauchillon g	Chair of the Board of Supervisors
For the California Department of Mental Healt	h:
Study a. Bajarian	
Stan Bajorin Chief Deputy Director (A) Department of Mental Health	
Exhibit A: Agreement between the Social California, Department of Mental Health with Guidelines for Federal, State and Local Ages the Social Security Administration".	n Attachment "Information System Security
ATTEST: Clerk of the Board of Supervisors	
By: Glad D. Cal	
APPROVED 7-21-09	APPROVED AS TO FORM
BOARD OF SUPERVISORS	Office of County Counsel
COUNTY OF NAPA ALADYS I. COIL	By:
CLERK OF THE BOARD	Date: