State of California—Health and Human Services Agency
Department of Health Care Services

SANDRA SHEWRY
Director

ARNOLD SCHWARZENEGGER
Governor

October 19, 2007

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY MEDI-CAL PROGRAM SPECIALISTS/LIAISONS
ALL COUNTY MEDS LIAISONS
ALL COUNTY INFORMATION SECURITY OFFICERS
ALL COUNTY PRIVACY OFFICERS

Letter No.: 07-20

SUBJECT: INFORMATION PRIVACY AND SECURITY ASSESSMENT

This letter instructs county welfare directors (Counties) to review their information privacy and security practices and report their findings to the Department of Health Care Services (Department) using an assessment questionnaire.

The federal Social Security Administration (SSA) is requiring the Department to conduct this information privacy and security assessment. The Department must comply with SSA requirements in order for the State and Counties to have continued access to SSA data related to Social Security beneficiary information.

Counties should refer to Attachment A for a copy of the information privacy and security assessment questionnaire. Counties must return the completed questionnaires to the Department by November 16, 2007.

BACKGROUND

The Department entered into a data sharing agreement with the SSA, effective July 1, 2007. The agreement limits access to SSA data to only authorized employees who need it to perform their official duties. The agreement contains security procedures relating to protecting the privacy of SSA Personally Identifiable Information (PII).

The agreement requires the Department to perform oversight of the SSA data being accessed by multiple users throughout the state who are agents and contractors of the

Department. The Department has developed language for agreements with the counties regarding the use of Medi-Cal PII (including SSA data). The language includes compliance requirements that meet SSA, as well as State and federal privacy and security requirements. Counties should refer to Attachment B for a copy of the draft Medi-Cal Information Privacy and Security Agreement.

ASSESSMENTS

The Department must regularly assess the Counties to monitor compliance with federal and State information privacy and security safeguards. The Department will perform these assessments by requiring all fifty-eight (58) Counties to complete the attached questionnaire and by also performing on-site assessments of six (6) Counties. The Department will individually contact the six (6) Counties which have been selected for on-site assessments and provide the scheduling and details of the on-site assessments. The Department will begin conducting the on-site assessments in October 2007 and conclude by December 31, 2007. Starting January 1, 2008, the Department will conduct on-site assessments in the remaining fifty-two (52) Counties.

QUESTIONNAIRE INSTRUCTIONS

Counties should report their level of compliance with the safeguards contained in the proposed Medi-Cal Information Privacy and Security Agreement using the attached assessment questionnaire.

The attached questionnaire has two parts.

- Part 1 is an information privacy and security assessment of the environment where Medi-Cal PII is used, stored, processed, or transmitted. Counties must complete this part once for their organization and return it to the Department by November 16, 2007. Counties must answer each question with a “yes” or “no” and detailed response as appropriate. The column titled “Evidence/Documents” advises Counties what the Department will expect for evidence/documentation during an on-site assessment or when the Department makes a request for evidence or documentation. “PII” means Personally Identifiable Information. PII is the information that can be used, alone or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files. Examples of PII may include but is not limited to: name, SSN, Social Security benefit data, date of birth, official State or government issued driver's

license or identification number. Counties should mail Part 1 using secured encrypted electronic media, such as an encrypted disc, or hardcopy to:

DHCS Privacy Office / Office of Legal Services
Attn: County Assessment Questionnaire
P.O. Box 997413, MS 0010
Sacramento, CA 95899-7413

- Part 2 instructs counties to assess written documentation of the system configuration and security features for each of the Counties' systems/applications that store/process/transmit Medi-Cal PII. The Department is not requesting information regarding the Medi-Cal Eligibility Data System (MEDS) in Part 2. Instead, the Department expects documentation on systems that may receive data from MEDS or other sources of Medi-Cal PII data. The Department may review the documentation during the Counties' on-site assessment. Counties should not send Part 2 documentation to the Department with the completed questionnaire. Counties should gather and retain these documents to give to Department personnel for review during on-site assessments, or should the Department contact Counties to request documentation pertaining to certain questions.

The Department appreciates Counties' efforts in completing this questionnaire. Compliance with SSA requirements will allow the Department and Counties to have continued access to mission-critical SSA data. The Department will contact the person identified as the responder in the event a questionnaire is not complete or there are questions regarding Counties' responses.

The Department will create a best practices document based upon information provided in the questionnaires and from the on-site assessments. The Department will provide all Counties with the best practices document shortly after conclusion of the six (6) on-site assessments.

If Counties have questions when completing the assessment questionnaire, or have knowledge of other county agencies that should complete a questionnaire, please contact

Ms. Diana Shelton of the Department's Privacy Office at (916) 440-7840 or at diana.shelton@dhcs.ca.gov.

Original Signed By

Vivian Auble, Chief
Medi-Cal Eligibility Division

Attachments

County Information Privacy and Security Assessment Questionnaire (Attachment A)

There are TWO (2) Parts to this Assessment Questionnaire.

- **Part 1** is an information privacy and security assessment of the environment where Medi-Cal PII is used, stored, processed, or transmitted. Complete this part ONCE for your organization and return it to DHCS.
- **Part 2 MAY BE REVIEWED DURING THE ON-SITE ASSESSMENT**
  For each of the systems/applications that store/process/transmit MEDI-CAL PII data, an assessment may be completed of the written documentation of the system configuration and system security features when DHCS conducts an on-site review.

Part 1

Instructions:

Enter your responses in the fields provided in the tables below. Answer every question.

Use the [TAB] key and [SHIFT]+[TAB] key to move forward and backward or use the mouse to select a field. Click on box field to check and uncheck.

If you need assistance please contact the DHCS Privacy Office Hotline - (916) 445-4646 or send your question via e-mail to privacyofficer@dhcs.ca.gov

You must return Part 1 of your completed questionnaire by November 16, 2007
Save Part 1 and mail it using secured encrypted electronic media or hardcopy to:
DHCS Privacy Office / Office of Legal Services
P.O. Box 997413, MS 0010
Sacramento, CA 95899-7413

COUNTY NAME:			
Information Security Officer:		**Phone:**	**Email:**
Privacy Officer:		**Phone:**	**Email:**

RESPONDER INFORMATION:			
Your Name:		**Phone:**	**Email:**
Organization Name:		**Position Title:**	
Organization /Entity Function:			
How long have you worked in this organization?	☐ **Less than 1 year**	☐ **1 to 2 years**	☐ **3 or more years**

County Facility Locations:

	Street Address	City	Zip code	Leased or Owned?	PROGRAMS AT THIS COUNTY FACILITY				
					Medi-Cal	TANF	MH	CWS/ CMS	Other Programs (please describe):
1.					☐	☐	☐	☐	☐
2.					☐	☐	☐	☐	☐
3.					☐	☐	☐	☐	☐
4.					☐	☐	☐	☐	☐
5.					☐	☐	☐	☐	☐
6.					☐	☐	☐	☐	☐
7.					☐	☐	☐	☐	☐
8.					☐	☐	☐	☐	☐
9.					☐	☐	☐	☐	☐
10.					☐	☐	☐	☐	☐
11.					☐	☐	☐	☐	☐
12.					☐	☐	☐	☐	☐
13.					☐	☐	☐	☐	☐
14.					☐	☐	☐	☐	☐
15.					☐	☐	☐	☐	☐

System Inventory List

Application/System Name	Contains Medi-Cal PII Data?		Primary function/purpose	Main Users	Application /System Custodian	Application /System Owner	Vendor (if applicable)	Change control procedures?		Disaster Recovery Plan?	
	Yes	No						Yes	No	Yes	No
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐
	☐	☐						☐	☐	☐	☐

SECTION I – Privacy and Confidentiality				
	YES	NO	Detailed Response:	Evidence / Documents
I.1. Do you have a general confidentiality policy relating to the use or disclosure of Medi-Cal PII?	☐	☐		▪ Policy Name and Number
I.2. How do you ensure that employees have access only to the minimum necessary Medi-Cal PII needed to do their jobs?				▪ Procedure
I.3. Have you identified the staff members or classes of persons who need access to Medi-Cal PII (electronic and paper) to carry out their duties?	☐	☐		▪ Job descriptions of staff that have access to Medi-Cal PII
I.4. Who uses Medi-Cal data and for what purpose or task(s)?				▪ Medi-Cal PII Secondary System Inventory ▪ Organizational structure
I.5. What is the estimated number of users that have access to Medi-Cal PII data?				▪ Log of all staff and contractors that have access to Medi-Cal PII
I.5.a. How many contractor staff have access?				
I.6. What kinds of requests are you receiving for Medi-Cal PII data?				▪ List of recent requests for Medi-Cal PII and purpose
I.7. What organizations/individuals are you releasing Medi-Cal PII data to?				▪ List of who Medi-Cal PII is being released to
I.8. Who is making the determination on what Medi-Cal PII data can be released and if the release is appropriate?				▪ Name/title of Individual(s)

SECTION II – Employee Training and Discipline				
	YES	NO	Detailed Response:	Evidence / Documents
II.1. Do you have a policy for sanctioning employees' non-compliance with preserving confidentiality and safeguarding confidential data?	☐	☐		▪ Policy Name and Number

SECTION II – Employee Training and Discipline				
	YES	NO	Detailed Response:	Evidence / Documents
II.1.a. Does the policy apply to all workforce members, including management, on-site contractors, consultants, temporary workers, volunteers, etc.?	☐	☐		▪ Example sanction
II.2. Have you trained all staff members that have access to Medi-Cal PII data on general information privacy and security?	☐	☐		▪ Number of staff trained ▪ Date of last training
II.3. Have you developed or acquired a privacy training tool?	☐	☐		
II.3.a. If so, please provide a description.				▪ Training Content Document
II.4. How many workforce members have access to Medi-Cal PII data and how many have been trained on your Information privacy and security Policies and Procedures?			# workforce w/access to Medi-Cal PII – # trained on Security and Privacy –	▪ Attendance Role
II.4.a. Is the training provided to temporary and contract staff the same as regular staff?	☐	☐		
II.4.b. Do you provide training for new staff?	☐	☐		
II.4.b.A. How often do you provide training?				▪ Employees Training History (multi-year)
II.4.b.B. How soon after hire?				
II.4.b.C. Before or after gaining access to Medi-Cal PII?				
II.5. Can you provide verification of training for each workforce member if requested?	☐	☐		▪ 3 year old training documentation
II.6. Do workforce members sign a certification after training agreeing to comply with privacy and security safeguards?	☐	☐		▪ Signed training certification
II.6.a. How often do they sign?				

SECTION III – Management Oversight and Monitoring				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
III.1. Has an Initial Risk Analysis been conducted to assess potential risks and vulnerabilities?	☐	☐		▪ Recent Risk Analysis Report
III.2. Have you implemented self-assessments to assist in maintaining compliance with privacy and security safeguards?	☐	☐		▪ Completed assessment documents
III.2.a. What is the frequency of these self-assessments?				▪ Date of last self-assessment
III.2.b. How long are copies of the self-assessments maintained?				
III.2.c. Who reviews the self-assessments?				▪ Name of person(s) responsible for reviewing self-assessments
III.2.d. Do you establish corrective action plans for each review and monitor all weaknesses until they are corrected?	☐	☐		
III.3. Who performs oversight/monitoring activities of compliance with privacy and security safeguards?				▪ List of people who conduct oversight and QA ▪ List primary duties of oversight and assessment teams.
III.4. Does your organization routinely include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts (RFO's)?	☐	☐		▪ RFO template
III.5. Do you randomly sample work activity including online access to Medi-Cal PII?	☐	☐		

SECTION IV – Confidentiality Statement and Background Check				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
IV.1. Are criminal history checks required as prerequisite to the hiring process and/or granting access to health information?	☐	☐		▪ Method/source for background checks ▪ Name of person responsible for background checks ▪ Hiring check-off sheet
IV.2. Are checks on temporary staff carried out either by contract with the temporary staffing agency or by the covered entity prior to allowing access to Medi-Cal PII?	☐	☐		
IV.3. Are employees asked to sign confidentiality or non-disclosure agreements as a part of the terms and conditions of employment? Does the agreement include:	☐	☐		▪ Signed Confidentiality Statement
IV.3.a. General Use	☐	☐		
IV.3.b. Security and Privacy Safeguards	☐	☐		
IV.3.c. Unacceptable Use	☐	☐		
IV.3.d. Enforcement Policies	☐	☐		
IV.4. Is there a recertification process in place to require employees to sign confidentiality or non-disclosure agreements occurring at specific intervals following the new hire process?	☐	☐		▪ Recertification Process and forms

SECTION V – Physical Security				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
V.1. How is access gained to the building?				
V.2. How is access gained to the working space?				
V.3. Is there a security guard at all locations where Medi-Cal PII is stored or used?	☐	☐		▪ Hours of patrol

SECTION V – Physical Security				
	YES	NO	Detailed Response:	Evidence / Documents
V.3.a. If so, what are the hours the guard is on duty (e.g. 24/7, work hours only, etc.)				
V.4. Are keys, locks, electronic or biometric devices required to gain access for sensitive areas such as server rooms/closets, archive rooms, and file rooms?	☐	☐		
V.5. Are keys, keycards and other access devices to facilities assigned and logged before they are disbursed?	☐	☐		▪ Sample log for a specifically requested date
V.5.a. Are they logged when they are retrieved?	☐	☐		
V.6. Are combination/cipher lock codes, card access codes, and/or lock cores changed when staff with knowledge of them leaves or no longer has a need to know them?	☐	☐		▪ Procedure
V.7. Are there security cameras at all locations where Medi-Cal PII is stored or used?	☐	☐		▪ Hours of operation ▪ How long tapes are stored
V.8. Are workers who assist in the administration of the Medi-Cal program provided identification badges?	☐	☐		
V.9. Is identification for visitors, maintenance personnel, consultants, and other contractors required throughout the facilities?	☐	☐		▪ Policy Name and Number
V.10. Is a record kept of all visitors, maintenance personnel, and others without authorized credentials that access the facility?	☐	☐		▪ Visitor log from specified date
V.11. Are visitors to areas where Medi-Cal PII is contained escorted and Medi-Cal PII kept out of sight while visitors are in the area?	☐	☐		

SECTION V – Physical Security				
	YES	NO	Detailed Response:	Evidence / Documents
V.12. Are portable devices such as laptops, disks, and thumb drives properly secured in the office? (Cable locked to desks? Locked in drawers?)	☐	☐		▪ Policy Name and Number
V.13. Is Medi-Cal PII left unattended on desks at any time during the day? Unattended means that information is not being observed by a worker authorized to access the information.	☐	☐		▪ Policy Name and Number
V.14. Is all Medi-Cal PII secured at the end of employees' shifts in locked drawers, cabinets, or file room?	☐	☐		
V.15. Are records with Medi-Cal PII left unattended at any time? Unattended means that information is not being observed by a worker authorized to access the information.	☐	☐		
V.16. Do employees have keys to desk drawers and overhead storage in their cubicle to store Medi-Cal PII?	☐	☐		
V.17. Do employees with offices have keys to their offices?	☐	☐		
V.17.a. Do employees keep keys with them at all times?	☐	☐		
V.18. Are computers, faxes and printers placed in areas that are easily accessible to unauthorized persons? (For example, are they in main hallways or offices or are they against back walls?)	☐	☐		▪ Policy Name and Number
V.19. Are printouts and faxes picked up regularly?	☐	☐		
V.20. Are workstations with access to Medi-Cal PII located in controlled areas?	☐	☐		
V.21. Are computer monitors that display Medi-Cal PII properly positioned to avoid inadvertent or unauthorized viewing?	☐	☐		▪ Policy Name and Number

SECTION V – Physical Security				
	YES	NO	Detailed Response:	Evidence / Documents
V.22. Is the area with servers, routers, and other computer equipment locked or otherwise secured?	☐	☐		
V.23. How is staff instructed to safeguard mobile media such as laptops, thumb drives, etc., containing Medi-Cal PII while in transit?				▪ Policy Name and Number ▪ Training material
V.24. Describe your method of disposal of media no longer needed by the organization.				▪ Policy Name and Number ▪ Procedure
V.25. Is mail that is kept overnight in the office secured in locked drawers, cabinets, or file room?	☐	☐		
V.26. Does this facility have fire detection and suppression devices/systems? (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) Please describe.	☐	☐		
V.27. Is the office cleaned during work hours or after hours?				
V.28. Who cleans the office, County staff or contract staff?				

SECTION VI – Computer Security Safeguards				
	YES	NO	Detailed Response:	Evidence / Documents
General Computer Security				
VI.1. Is an overall security plan developed that provides an overview of the security requirements and a description of the security controls in place or planned for meeting those requirements?	☐	☐		▪ Security plan

SECTION VI – Computer Security Safeguards				
	YES	NO	Detailed Response:	Evidence / Documents
VI.2. Does the system support virus protection?	☐	☐		▪ Product and licenses Name of those that administrate AV software ▪ Individual(s) responsible for responding to infection
VI.3. Are newly released security relevant patches, service packs, and hot fixes applied in an expeditious manner?	☐	☐		▪ Inventory of Servers, and PC's showing latest patches
VI.4. Media reuse				
VI.4.a. What policies for the re-use of media and devices that previously contained Medi-Cal PII are established?				▪ Policy Name and Number
VI.4.b. Is there a documented methodology to clean media prior to re-use?	☐	☐		▪ Product used ▪ Person responsible ▪ List of recent systems wiped ▪ Procedure for identifying systems to be wiped
VI.4.c. Is damaged media stored and/or destroyed?	☐	☐		
VI.5. Does the system prevent user from seeing and printing menu items, screen formats, report forms if user's security profile prevents them from access in the data elements associated with these system components?	☐	☐		
VI.6. Does the organization have a policy on telecommuting?	☐	☐		▪ Policy Name and Number
VI.7. Do workers access Medi-Cal PII remotely?	☐	☐		
VI.8. Do you have a password policy?	☐	☐		▪ Policy
VI.8.a. Briefly describe your password requirements/restrictions.				

SECTION VI – Computer Security Safeguards				
	YES	NO	Detailed Response:	Evidence / Documents
VI.9. Are workforce members required to change passwords on a regular basis?	☐	☐		▪ Password renewal policy
VI.9.a. What is the frequency?				
VI.10. Are privileged accounts such as root, admin and system administration, required to change passwords on a regular basis?	☐	☐		▪ Password renewal policy
VI.10.a. What is the frequency?				
VI.11. How are passwords to new users distributed?				▪ Procedure
VI.12. Does your organization use digital encryption?	☐	☐		▪ Encryption products used & number of licenses
VI.12.a. If the organization does not use encryption, does it use another mechanism for access control to ensure that only authorized individuals can gain access?	☐	☐		▪ Controls used
VI.12.b. Are disks, thumb drives, and other portable media used by staff?	☐	☐		▪ Process for requesting authorization of portable media with Medi-Cal PII.
VI.12.b.A. If so, are they encrypted?	☐	☐		
VI.12.c. If you have a mobile workforce, do you require encryption for laptops?	☐	☐		▪ Encryption products used & number of licenses
VI.12.d. Are workstations which store or process Medi-Cal PII encrypted?	☐	☐		▪ Encryption products used & number of licenses
VI.13. Do you ensure that only the minimum necessary amount of Medi-Cal PII may be downloaded to a laptop or hard drive when absolutely necessary for current business purposes?	☐	☐		▪ Controls used ▪ List of authorized downloads ▪ Forms & process for requesting approval
VI.14. Is Medi-Cal PII sent via e-mail?	☐	☐		▪ Examples of MPII sent via e-mail

SECTION VI – Computer Security Safeguards				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
VI.14.a. If so, is encryption utilized?	☐	☐		▪ Availability to encryption by Medi-Cal PII workforce
VI.14.a.A. If so, what solution is implemented?				▪ Encryption product & license
VI.14.a.B. How are staff trained to use this tool?				▪ Training covering need and process for encrypting emails
VI.15. Is Medi-Cal PII downloaded, exported or otherwise extracted into spreadsheets or local databases?	☐	☐		
VI.15.a. For what purpose is this done?				
VI.16. How is data wiped from the system?				
System Security Controls				
VI.17. Are Identification codes used only to represent one person?	☐	☐		
VI.18. Does the system require the use of both a user identification code and password to verify authorization to access the system?	☐	☐		
VI.19. Do you have the capability to produce reports monitoring user successful and unsuccessful login attempts?	☐	☐		▪ Sample report
VI.20. Does the application automatically lock the account until released by an administrator when the maximum number of unsuccessful login attempts is exceeded?	☐	☐		▪ Policy Name and Number
VI.20.a. What are the maximum login attempts?				
VI.21. Does the system have mechanisms for automatic logoff or timeout?	☐	☐		▪ Description of how this is implemented
VI.21.a. What is the length of time for logoff or timeout to appear?				

SECTION VI – Computer Security Safeguards				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
VI.22. Is a warning banner displayed stating that data is confidential, systems are logged, system use is for business purposes only and directing user to log off the system if they do not agree with these requirements?	☐	☐		▪ Screen copy of Warning Banner
VI.23. Does the system allow defining access to specific data elements, files, functions, menus, commands, and networks based on user's responsibilities or job function, such as the examples below: • Business Systems Analyst • System Administrator • Technical (programmer or Vendor) • Data Center Operations Personnel • IT Manager/Supervisor • End-user – accessing Medi-Cal PII • End-user – no access to Medi-Cal PII	☐	☐		
VI.24. Do you have firewalls in place to protect your internal network? (describe what is used and where it is placed)	☐	☐		▪ Architecture Diagram ▪ Security and Access Middleware ▪ Technical Resource
VI.25. Is activity logged (data access, data changes, system access, and system changes)?	☐	☐		▪ Description of what is logged
VI.25.a. How long are these logs maintained?				
VI.25.b. Who monitors these logs?				▪ Individual(s) responsible for monitoring logs
VI.26. Does the system provide control over stored data to ensure data is complete and internally consistent?	☐	☐		
VI.27. Is security testing, including intrusion testing, performed regularly on systems and networks?	☐	☐		▪ Intrusion Detection Product(s)
VI.28. Are data transmissions containing Medi-Cal PII encrypted?	☐	☐		▪ Encryption products used & number of licenses

SECTION VI – Computer Security Safeguards				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
Audit Controls				
VI.29. Do you have an access control policy and procedure?	☐	☐		▪ Policy Name and Number ▪ Procedure
VI.30. Are access authorizations documented and maintained?	☐	☐		▪ Completed forms used to request and authorize level of access.
VI.31. What is the procedure to modify access when it is required?				▪ Process for changing access when worker is reassigned or terminated.
VI.32. What is the mechanism by which access is terminated for individuals who no longer need access to Medi-Cal PII?				▪ Procedure
VI.32.a. How quickly is access termination completed and documented?				
VI.32.b. How are access termination requests communicated to the appropriate departments?				▪ Procedure
VI.33. What are the procedures for authorization to allow remote access?				▪ Policy Name and Number
VI.33.a. Who authorizes remote access?				
VI.33.b. What methods do you use for remote access? (e.g., VPN, broadband, dial up)				
VI.33.c. Describe security controls				
VI.34. How often are inactive accounts reviewed?				▪ Name/title of individual(s) reviewing inactive accounts

SECTION VI – Computer Security Safeguards				
	YES	NO	Detailed Response:	Evidence / Documents
VI.35. Are disabled accounts permanently deleted after a specified period?	☐	☐		▪ Threshold for deleting
VI.36. Are system administration functions separate from system operation, management, and maintenance functions?	☐	☐		
VI.37. Do you have the capability to produce reports that capture information about transaction usage patterns among authorized users for monitoring typical usage patterns compared to extraordinary usage?	☐	☐		▪ Sample report
VI.38. Has a procedure been established to review system logs for unauthorized access?	☐	☐		▪ Procedure
VI.39. Are requests for SSA or MEDS information monitored?	☐	☐		▪ List of recent requests for SSA or Meds data
VI.39.a. Who is responsible for authorizing requests for SSA or MEDS information?				▪ Name/Title of individual(s) responsible for authorizing requests
VI.40. Have you established a change control procedure for all systems containing Medi-Cal PII?	☐	☐		▪ Policy Name and Number
VI.40.a. What is your protocol for making emergency changes?				▪ Emergency Change Request procedure
VI.41. Do systems containing Medi-Cal PII have audit trails established to monitor activity?	☐	☐		▪ Policy Name and Number
VI.42. Generally, how often do you conduct a system security review?				

SECTION VI – Computer Security Safeguards				
	YES	NO	Detailed Response:	Evidence / Documents
Business Continuity / Disaster Recovery Controls				
VI.43. Does your organization have a Disaster Recovery Plan?	☐	☐		▪ Copy of Disaster Recovery Plan ▪ Policy Name and Number & Procedure for initiating a disaster recovery operation ▪ Policy Name and Number that covers requirement for a DR plan ▪ Names of workers responsible for the DR plan.
VI.44. Does your organization have a Business Continuity Plan?	☐	☐		▪ Policy Name and Number that covers requirement for a BC plan ▪ Policy Name and Number & Procedure for initiating a Business Continuity operation

SECTION VII – Paper Document Controls				
	YES	NO	Detailed Response:	Evidence / Documents
VII.1. Are paper documents (Medi-Cal PII) destroyed when no longer needed? HOW? (e.g., shredders, confidential destruct bins, boxes, etc.)	☐	☐		▪ Policy Name and Number
VII.2. Is a staff assigned to regularly check for faxes and deliver them to addressees?	☐	☐		
VII.3. Are fax numbers cross-verified before faxing?	☐	☐		▪ Policy Name and Number

SECTION VII – Paper Document Controls				
	YES	NO	Detailed Response:	Evidence / Documents
VII.4. Do faxes contain a confidentiality statement?	☐	☐		▪ Copy of Confidentiality Statement
VII.5. How is Medi-Cal PII mailed – US postal service, FedEx, UPS, courier?				▪ Policy Name and Number
VII.5.a. Is an inventory kept as to what was mailed to whom and when?	☐	☐		▪ Copy of recent mail log
VII.5.b. Is there a return receipt requested or mail tracking system?	☐	☐		
VII.5.c. Are discs with confidential information encrypted when sent through the mail?	☐	☐		▪ Policy Name and Number
VII.5.d. Is there internal/external labeling for sensitivity?	☐	☐		
VII.5.e. Is there external labeling with special handling instructions?	☐	☐		
VII.6. Who authorizes transport of Medi-Cal PII off the County premises and for what purposes?				▪ Name/Title of individual authorizing
VII.7. Where are Medi-Cal PII stored?				▪ Contracts for storage ▪ Name of Companies and locations
VII.7.a. Active files				
VII.7.b. Closed files				
VII.7.c. Archived files				

SECTION VIII – Notification and Investigation of Breaches				
	YES	NO	Detailed Response:	Evidence / Documents
VIII.1. Do you have policies and procedures that address identifying and responding to suspected or known security incidents, mitigating the incident, and documentation of security incidents and their outcomes?	☐	☐		▪ Policy Name and Number

SECTION VIII – Notification and Investigation of Breaches				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
VIII.2. Have you established criteria for what constitutes a security incident?	☐	☐		▪ Criteria list ▪ Incident types
VIII.3. To whom are you reporting security incidents?				▪ Name/Title of individuals
VIII.4. Is a log of all security incidents maintained and periodically reviewed by management?	☐	☐		▪ Name/title of individual(s) reviewing incidents ▪ Recent Log of incidents
VIII.5. Under what circumstances do you notify individuals of breach or unauthorized use or disclosure?				

SECTION IX– Compliance with SSA Agreement				
	YES	**NO**	**Detailed Response:**	**Evidence / Documents**
IX.1. Have you implemented self-assessments to assist in maintaining compliance with • **1137 – Information Exchange Agreement** the Agreement between the Social Security Administration and DHCS • **The Federal Information Security Management Act (FISMA)** • **Information System Security Guidelines For Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration**	☐	☐		
IX.1.a. What is the frequency of these self-assessments?				
IX.1.b. When was the last self-assessment completed?				▪ Date of last self-assessment
IX.1.c. How long are copies of the self-assessments maintained?				

SECTION IX– Compliance with SSA Agreement				
	YES	NO	Detailed Response:	Evidence / Documents
IX.1.d. Who reviews the self-assessments?				▪ Name/title of individual(s) reviewing self-assessments
IX.1.e. Do you establish corrective action plans for each review and monitor all weaknesses until they are corrected?	☐	☐		▪ Copy of recent corrective action plan following a self-assessment

SECTION X– Compliance by County Contractors/Agents				
	YES	NO	Detailed Response:	Evidence / Documents
X.1. Have all County Contractors/Agents that have access to Medi-Cal PII been identified?	☐	☐		▪ List of County Contractors/Agents that have access to Medi-Cal PII
X.2. Is there a signed agreement with each County Contractor/Agent that has access to Medi-Cal PII?	☐	☐		▪ Sample agreement
X.2.a. Does the agreement require the County Contractors/Agents to implement and maintain administrative, physical and technical safeguards?	☐	☐		
X.2.b. Does the agreement define “security incidents” and does it specify security incident reporting procedures?	☐	☐		

PART 2

THIS PART MAY BE REVIEWED DURING THE ON-SITE ASSESSMENT

FOR EACH OF THE SYSTEMS/APPLICATIONS THAT STORE/PROCESS/TRANSMIT MEDI-CAL PII DATA

DHCS MAY REVIEW ON-SITE THE FOLLOWING
WRITTEN DOCUMENTATION OF THE SYSTEM CONFIGURATION AND SYSTEM SECURITY FEATURES

At a minimum documentation should include:

1. A general description of the major hardware and software platforms currently in use, including a description of the system's security design features and user access control
2. A general description of the telecommunications environment applicable to the system including a description of the security and encryption protocols utilized for secure transmission of Medi-Cal PII.
3. A description of the number and type of contractor employees that will have access to the Medi-Cal PII contained in this system.
    a. The circumstances under which contractors would be granted such access.
    b. An explanation of the systematic controls and audit tracking capability regarding access to Medi-Cal PII.
4. Contractual language governing the relationship between the County's system, its contractors and their employees that indicates the penalties for inappropriate use of Medi-Cal PII within or passing through the County's system.

ATTACHMENT B

MEDI-CAL DATA PRIVACY AND SECURITY AGREEMENT

The California Department of Social Services (CDSS) and the California Department of Health Care Services (DHCS) have entered into a number of agreements wherein CDSS has agreed to provide services through the counties to DHCS in exchange for payment of Title XIX funds. In addition, local assistance funds are provided directly to the counties under Title XIX in exchange for the counties' assistance in the administration of the California Medi-Cal program.

Because of concerns about the privacy and security of confidential Medi-Cal data, known herein as personally identifiable information (PII), and because certain federal agencies have required DHCS to enter into agreements promising to protect the privacy and security of federal data as a condition to the receipt of that data, DHCS and the County of _____ (hereinafter "COUNTY") hereby enter into this Medi-Cal Data Privacy and Security Agreement.

In this Agreement Medi-Cal PII is information that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify 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.

I.
Privacy and Confidentiality

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. COUNTY eligibility workers may use or disclose Medi-Cal PII only to determine eligibility for individuals applying for Medi-Cal. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. COUNTY workers participating in the InHome Supportive Services (IHSS) program may use or disclose Medi-Cal PII only to perform administrative functions essential to the operation of the IHSS program. Any other use of 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, including to health care providers and law enforcement.

Access to Medi-Cal PII shall be restricted to only workers who need the Medi-Cal PII to perform their official duties in connection with the administration of the Medi-Cal program.

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.
Employee Training and Discipline

COUNTY agrees to advise all workers who will 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, COUNTY agrees as follows:

1. To train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII; and discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment. In complying with this requirement, COUNTY shall do the following:

2. Provide privacy and security awareness training to each new worker within 30 days of employment and thereafter at least annually to all workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII.

3. Require each worker who receives privacy and information security awareness training to sign a certification annually, indicating the worker's name and the date on which the training was completed.

4. Retain each worker's written certifications for inspection for a period of three years.

III.
Management Oversight and Monitoring

COUNTY agrees to 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 data.

COUNTY agrees that ongoing management oversight shall include periodic self-assessments and randomly sampling work activity, including on-line access to Medi-Cal and federal data by workers who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII.

COUNTY agrees that these management oversight and monitoring activities shall be performed by workers whose job functions are separate from those who use or disclose Medi-Cal PII as part of their official duties.

IV.
Confidentiality Statement and Background Check

COUNTY agrees to comply with the following requirements:

1. All workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII shall 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 the worker prior to access to Medi-Cal PII. The statement shall be renewed annually.

2. Before a worker may access Medi-Cal PII, County shall conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data.

V.
Physical Security

COUNTY agrees that Medi-Cal PII shall be used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours.

COUNTY agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure.

COUNTY agrees to comply with the following physical security safeguards:

1. All COUNTY facilities where workers assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII shall be secure facilities accessed only by authorized workers with properly coded key cards, authorized door keys or access authorization and access to premises is by official identification.

2. There shall be a security guard force 24 hours a day, 7 days a week at COUNTY facilities where Medi-Cal PII is stored or used.

3. Workers who assist in the administration of the Medi-Cal program shall be provided with badges.

4. Records with Medi-Cal PII shall be stored in spaces which are locked, such as file cabinets, file rooms, desks or offices. Records with Medi-Cal PII shall not be left unattended. Unattended means that information is not being observed by a worker authorized to access the information. Records with Medi-Cal PII shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

5. Visitors to areas where Medi-Cal PII is contained shall be escorted and Medi-Cal PII shall be kept out of sight while visitors are in the area.

VI.
Computer Security Safeguards

COUNTY agrees to comply with the following safeguards:

General Computer Security

1. All workstations and laptops that process and/or store Medi-Cal PII shall be encrypted with a DHCS approved solution or a solution using a vendor product specified on the California Strategic Sourced Initiative (CSSI) located at the following link: www.pd.dgs.ca.gov/masters/EncryptionSoftware.html

2. Only the minimum necessary amount of Medi-Cal PII may be downloaded to a laptop or hard drive when absolutely necessary for current business purposes.

3. All electronic files that contain Medi-Cal PII shall be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) with a DHCS approved solution or a solution using a vendor product specified on the CSSI.

4. All emails that include Medi-Cal PII shall be sent via an encrypted method using a DHCS approved solution or a solution using a vendor product specified on the CSSI.

5. All workstations, laptops and other systems that process and/or store Medi-Cal PII shall have a commercial third-party anti-virus software solution with a minimum daily automatic update.

6. All workstations, laptops and other systems that process and/or store Medi-Cal PII shall have current security patches applied.

7. All users shall be issued a unique user name for accessing Medi-Cal PII. Passwords shall not be shared. Passwords shall be at least eight characters. and shall be a non-dictionary word. Passwords shall not be stored in readable format on the computer. Workers shall not write down or post passwords or include passwords in a data file, log-on script or macro. Passwords shall be changed every 60 days. Passwords shall be changed if revealed or compromised. Any suspected unauthorized use of an ID or password shall be reported to the supervisor or county security officer immediately. Passwords shall be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

8. All Medi-Cal PII shall be wiped from systems when the data is no longer necessary. The wipe method must conform to Department of Defense standards for data destruction.

9. Any remote access to Medi-Cal PII shall be executed over an encrypted method approved by DHCS or using a vendor product specified on the CSSI. All remote access shall be limited to minimum necessary and least privilege principles.

System Security Controls

10. All systems containing Medi-Cal PII shall physically and logically isolate Medi-Cal PII from access by unauthorized users and other systems or applications. Medi-Cal PII shall not be accessed directly by computer but only through an application middleware that will authenticate and validate all data requests and users. All user data input shall be validated before being committed to the databases. All accesses and requests for data shall be logged and audited regularly. These controls shall be documented and approved by DHCS.

11. All systems containing Medi-Cal PII shall provide an automatic timeout after 20 minutes of inactivity.

12. All systems containing Medi-Cal PII shall 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.

13. All systems containing Medi-Cal PII shall log successes and failures of user authentication and authorizations granted. The system shall log all activities (data access, data changes, system access, and system changes) within the system conducted by all users (including all levels of users, system administrators, developers, and auditors). These logs shall be maintained for a period of at least three (3) years and shall be monitored regularly for anomalies.

14. All systems containing Medi-Cal PII shall use role based access controls for all user authentication, enforcing the principle of least privilege.

15. All data transmissions shall be encrypted end-to-end using a DHCS approved solution or a solution using a vendor product specified on the CSSI,

when processing and/or storing Medi-Cal PII. Medi-Cal PII shall be encrypted at the minimum of 128K AES or 3DES (Triple DES) if AES is unavailable.

16. All systems that are accessible via the Internet or store Medi-Cal PII shall actively use a comprehensive third-party real-time host based intrusion detection and prevention program.

Audit Controls

17. All systems processing and/or storing Medi-Cal PII shall have at least an annual system security review. Reviews shall include administrative and technical vulnerability scanning tools.

18. All systems processing and/or storing Medi-Cal PII shall have a routine procedure in place to review system logs for unauthorized access. Logs shall be maintained for a minimum of three years after the occurrence.

19. An automated audit trail record identifying either the individual worker or the system process that initiated a request for information from the Social Security Administration (SSA) shall be maintained. In addition, an automated audit trail record shall be maintained of all MEDS users. 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 the 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.

20. COUNTY in conjunction with DHCS shall exercise management control and oversight 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.

21. COUNTY shall monitor in order to routinely detect anomalies in the volume and/or type of queries requested by individual workers, and procedures for verifying that requests for SSA or MEDS information are in compliance with valid official business purposes. Systems shall produce reports providing supervisors with the capability to appropriately monitor user activity, such as ID exception reports, inquiry match exception reports, system error exception reports, and inquiry activity statistical reports.

22. All systems processing and/or storing Medi-Cal PII shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

Business Continuity / Disaster Recovery Controls

23. COUNTY shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Medi-Cal PII in the event of an emergency.

24. COUNTY shall have established documented procedures to backup Medi-Cal PII to maintain retrievable exact copies. The plan shall include a regular schedule for making backups, storing backups offsite, an inventory of backup tapes, the amount of time to restore Medi-Cal PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Medi-Cal PII.

VII.
Paper Document Controls

COUNTY agrees to comply with the following safeguards:

1. Medi-Cal PII in paper form shall be disposed of through confidential means, such as cross cut shredding and pulverizing.

2. Medi-Cal PII shall not be removed from the premises of the County except with express permission of DHCS.

3. Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified before sending.

4. Medi-Cal PII shall only be mailed using secure methods. Large volume mailings of Medi-Cal PII shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail shall be encrypted with a DHCS approved solution or a solution using a vendor product specified on the CSSI.

VIII.
Notification and Investigation of Breaches

1. COUNTY agrees to notify DHCS immediately by telephone call or e-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 discovery of any other suspected security incident, intrusion, loss or unauthorized use or disclosure of PII in violation of this Agreement or the law. Notification shall be provided to the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident

occurs after business hours or on a weekend or holiday and involves electronic PII, notification shall be provided by calling the DHCS ITSD Help Desk.

2. Initial notification shall include contact and component information; a description of the breach or loss with scope, numbers of files or records, type of equipment or media, approximate time and location of breach or 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 organizations been contacted; and whether any other reports have been filed.

3. COUNTY shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment.

4. COUNTY shall investigate the breach and produce a written breach report within ten working days of the incident, detailing what data elements were involved; a description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PII; a description of where PII is believed to have been improperly transmitted, sent, or used; a description of the probable causes of the breach; detailed corrective action plan including measures that were taken to halt and/or contain the breach. The breach report shall be sent to the DHCS Privacy Officer and Information Security Officer.

5. COUNTY shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and pay costs of such notifications, as well as any costs associated with the breach. The DHCS Privacy Officer shall approve the time, manner and content of any such notifications.

IX.
Compliance with SSA Agreement

In addition to the above, COUNTY agrees to comply with all substantive privacy and security requirements in the Agreement between the Social Security Administration and DHCS, known as the 1137 Agreement, which is appended to and hereby incorporated into this Agreement.

X.
Compliance by COUNTY Agents

COUNTY also agrees to ensure that any agents, including subcontractors, which assist COUNTY in its Medi-Cal functions and to which COUNTY provides PII, agree to the same privacy and security safeguards as are contained in this Agreement; and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or subaward to such agents or subcontractors.

XI.
Assessments and Reviews

In order to enforce this Agreement and ensure compliance with its provisions, COUNTY agrees to allow DHCS to inspect the facilities, systems, books and records of COUNTY in order to perform assessments and reviews. COUNTY also agrees to promptly remedy any violation of any provision of this Agreement and certify the same to the DHCS Privacy Officer and Information Security Officer in writing.

XII.
Sanctions and Penalties

Failure to remedy serious violations of this Agreement, or serious breaches under this Agreement may cause DHCS to suspend the flow of data to COUNTY and/or suspend payments to COUNTY for assisting in the administration of the Medi-Cal program.

XIII.
Assistance in Litigation or Administrative Proceedings

COUNTY shall make itself and any subcontractors, agents, and workers assisting in the administration of the Medi-Cal program and using or disclosing Medi-Cal PII available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings involving DHCS based upon claimed violations of the privacy or security of Medi-Cal PII, federal or state laws or agreements.

XIV.
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. The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement effective this _____ day of _____, 2007.

For COUNTY:

_____

(Name)
(Title)

For CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

Stan Rosenstein
Chief Deputy Director- Health Care Programs

Attachment: Agreement between the Social Security Administration and the State of California, Department of Health Care Services with Attachment "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration".