MEDI-CAL PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California
Department of Health Care Services and the

County of _____, _____,

Department/Agency of _____

_____.

PREAMBLE

The Department of Health Care Services (DHCS) and the

County of

_____

,

Department/Agency of _____

_____

(County Department) enter into this Medi-Cal Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (Medi-Cal PII).

DHCS receives federal funding to administer California's Medicaid Program (Medi-Cal). The County Department/Agency assists in the administration of Medi-Cal, in that DHCS and the County Department/Agency access DHCS eligibility information for the purpose of determining Medi-Cal eligibility.

This Agreement covers the ~~County of ,~~ ~~Department of~~

County of

_____

, _____

Department/Agency of _____

workers, who assist in the administration of Medi-Cal; and access, use, or disclose Medi-Cal PII.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. **"Assist in the administration of the Medi-Cal program"** means performing administrative functions on behalf of Medi-Cal, such as establishing eligibility,

determining ~~eligibility for, or enrollment in, or~~ the amount of~~, public benefits~~ medical assistance, and collecting Medi-Cal PII for such purposes, to the extent such activities are authorized by law.

2. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized-purposes have access or potential access to Medi-Cal PII, whether electronic, paper, verbal, or recorded.

3. **"County Worker"** means those county employees, contractors, subcontractors, vendors and agents performing any functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII.

4. **"Medi-Cal PII"** is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual. Medi-Cal PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. Medi-Cal PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. Medi-Cal PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

   ~~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, paper, verbal, or recorded.~~

5. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Medi-Cal PII, or interference with system operations in an information system which processes Medi-Cal PII that is under the control of the County or County's Statewide Automated Welfare System (SAWS) Consortium, or a contractor, subcontractor or vendor of the County.

6. **"Secure Areas"** means any area where:
   A. County Workers assist in the administration of Medi-Cal;
   B. County Workers use or disclose Medi-Cal PII; or
   C. Medi-Cal PII is stored in paper or electronic format.

7. **"SSA-provided or verified data (SSA data)"** means:
   A. Any information under the control of the Social Security Administration (SSA) provided to DHCS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or

B. Any information provided to DHCS, including a source other than SSA, but in which DHCS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

For a more detailed definition of "SSA data", please refer to Section 7 of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

AGREEMENTS

~~**NOW THEREFORE**,~~ DHCS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. ~~The~~ County Department ~~workers covered by this Agreement (~~/Agency County Workers~~)~~ may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal in accordance with Section 14100.2 of the Welfare and Institutions Code ~~section 14100.2 and~~ , Section 431.300 et. Seq. of Title 42 Code of Federal Regulations ~~section 431.300 et.seq., or~~ , and as otherwise required by law. Disclosures~~, which are~~ required by law~~, such as a court order, or~~ or that are made with the explicit written authorization of ~~the~~a 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. Pursuant to this Agreement, County Workers may only use Medi-Cal PII to ~~perform administrative functions related to determining eligibility for individuals applying for Medi-Cal~~assist in the administration of the Medi-Cal program.

C. Access to Medi-Cal PII shall be restricted to County Workers who need to perform their official duties to assist in the administration of Medi-Cal.

D. 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. PERSONNEL CONTROLS

The County Department/Agency 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/Agency shall implement the following personnel controls:

A. ***Employee Training***. Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:

1. Provide initial privacy and security awareness training to each new County Worker within 30 days of employment ~~and~~;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three or more security reminders per year are recommended;

3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed and;

4. Retain training records for a period of three years after completion of the training.

B. ***Employee Discipline***.

1. Provide documented sanction policies and procedures for County Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.

2. Sanction policies and procedures shall include termination of employment when appropriate.

C. ***Confidentiality Statement***. Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three years, or five years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document, an attachment of Exhibit A.

The statement shall include, at a minimum, a description of the following:

1. General Use of Medi-Cal PII;

2. Security and Privacy Safeguards for Medi-Cal PII;

3. Unacceptable Use of Medi-Cal PII; and

4. Enforcement Policies.

D. ***Background Screening***.

1. Conduct a background screening of a County Worker before they may access Medi-Cal PII.

2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3. The County Department/Agency shall retain each County Worker's background screening documentation for a period of three years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

To ensure compliance with the privacy and security safeguards in this Agreement the county shall perform the following:

A. Conduct periodic privacy and security review of work activity by County Workers, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of Medi-Cal PII.

B. The periodic privacy and security reviews ~~must~~shall be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of the Medi-Cal program, and the use or disclosure of Medi-Cal PII.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County Department/Agency agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

B. Provide the DHCS with applicable contact information for these designated

individuals using the County PSA inbox listed in Section XI of this Agreement. Any changes to this information should be reported to DHCS within ten days.

~~B.~~C. Assign ~~county workers~~County Workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

The County Department/Agency shall ensure Medi-Cal PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The County Department/Agency agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of the County Department/Agency facilities where County Workers assist in the administration of Medi-Cal and use, disclose, or store Medi-Cal PII.

B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
   1. Properly coded key cards
   2. Authorized door keys
   3. Official identification

C. Issue identification badges to County Workers.

D. Require County Workers to wear these badges where Medi-Cal PII is used, disclosed, or stored.

E. Ensure each physical location, where Medi-Cal PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

F. Ensure there are security guards or a monitored alarm system at all times at the County Department/Agency facilities and leased facilities where 500 or more individually identifiable records of Medi-Cal PII is used, disclosed, or stored. Video surveillance systems are recommended.

G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of Medi-Cal PII have perimeter security and physical access controls that limit access to only authorized County Workers. Visitors to the data center area ~~must~~shall be escorted at all times by authorized County Workers.

H. 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 which

are multi-use meaning that there are County Department/Agency and non-County Department/Agency functions in one building in work areas that are not securely segregated from each other. It is recommended that all Medi-Cal PII be locked up when unattended at any time, not just within multi-use facilities.

A. The County Department/Agency shall have policies that include, based on applicable risk factors that include, at a minimum, a description of the circumstances under which the County Workers

H.I. can transport Medi-Cal PII, as well as the physical security requirements during transport. A County Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles mustshall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit Medi-Cal PII be left unattended in a vehicle overnight or for other extended periods of time.

I.J. The County Department/Agency shall have policies that indicate County Workers are not to leave records with Medi-Cal PII unattended at any time in airplanes, buses, trains, etc., includinginclusive of baggage areas. This should be included in training due to the nature of the risk.

VI. TECHNICAL SECURITY CONTROLS

A. ***Workstation/Laptop Encryption***. All workstations and laptops, which use, store and/or process Medi-Cal PII, mustshall be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution mustshall be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

B. ***Server Security***. Servers containing unencrypted Medi-Cal PII mustshall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

C. ***Minimum Necessary***. Only the minimum necessary amount of Medi-Cal PII required to perform required business functions may be accessed, copied, downloaded, or exported.

D. ***Mobile Device and Removable Media***. All electronic files, which contain Medi-Cal PII data, must, shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones,

tablets, backup tapes etc.). Encryption ~~must~~shall be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

E. ***Antivirus Software***. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, ~~must~~shall install and actively use an anti-virus software solution. Anti-virus software should have automatic updates for definitions scheduled at least daily.

F. ***Patch Management***.

1. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, ~~must~~shall have critical security patches applied, with system reboot if necessary.

2. There ~~must~~shall be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.

3. At a maximum, all applicable patches deemed as critical ~~must~~shall be installed within 30 days of vendor release. It is recommended that critical patches which are high risk be installed within ~~seven~~7 days.

4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, ~~must~~shall have compensatory controls implemented to minimize risk.

G. ***User IDs and Password Controls***.

1. All users ~~must~~shall be issued a unique user name for accessing Medi-Cal PII.

2. ~~Username must~~Usernames shall be promptly disabled, deleted, or the password changed ~~upon~~within, at most, 24 hours of the transfer or termination of an employee~~, at maximum within 24 hours~~.

3. Passwords are not to be shared.

4. Passwords ~~must~~shall be at least eight characters.

5. Passwords ~~must~~shall be a non-dictionary word.

6. Passwords ~~must~~shall not be stored in readable format on the computer or server.

7. Passwords ~~must~~shall be changed every 90 days or less. It is

recommended that passwords be required to be changed every 60 days or less.
Non-expiring passwords are permitted when in full compliance with NIST SP 800-63B Authenticator Assurance Level (AAL) 2.

8. Passwords ~~must~~shall be changed if revealed or compromised.

9. Passwords ~~must~~shall be composed of characters from at least three of the ~~following~~ four groups from the standard keyboard:

   a. Upper case letters (A-Z)
   b. Lower case letters (a-z)
   c. Arabic numerals (0-9)
   d. Special characters

H. ***User Access***. In conjunction with DHCS, management should exercise control and oversight, of the function of authorizing individual user access to ~~Social Security Administration (~~

SSA~~)~~ data~~,~~ via Medi-Cal Eligibility Data System (MEDS), and over the process of issuing and maintaining access control numbers, IDs, and passwords.

~~H.~~I. ***Data Destruction***. When no longer needed, all Medi-Cal PII ~~must~~shall be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Medi-Cal PII cannot be retrieved.

~~I.~~J. ***System Timeout***. The systems providing access to Medi-Cal PII ~~must~~shall provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

~~J.~~K. ***Warning Banners***. The systems providing access to Medi-Cal PII ~~must~~shall display a warning banner stating, at a minimum:

1. Data is confidential;

2. Systems are logged;

3. System use is for business purposes only, by authorized users; and

4. Users shall log off the system immediately if they do not agree with these requirements.

~~K.~~L. ***System Logging***.

1. The systems ~~which~~that provide access to Medi-Cal PII ~~must~~shall maintain an automated audit trail that can identify the user or system

process which initiates a request for Medi-Cal PII, or alters Medi-Cal PII.

2. The audit trail shall:

   a. Be date and time stamped;
   b. Log both successful and failed accesses;
   c. Be read-access only; and
   d. Be restricted to authorized users of the audit trail.

3. If Medi-Cal PII is stored in a database, database logging functionality shall be enabled.

4. Audit trail data shall be archived for at least three years from the occurrence.

~~L.~~M. ***Access Controls***. The system providing access to Medi-Cal PII shall use role based access controls for all user authentications, enforcing the principle of least privilege.

~~M.~~N. ***Transmission Encryption***.

1. All data transmissions of Medi-Cal PII outside of a secure internal network ~~must~~shall be encrypted using a FIPS 140-2 certified algorithm that is 128 bit or higher, such as AES or TLS. It is encouraged, when available and when feasible, that 256 bit encryption be used.

2. Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted.

3. This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and email.

~~N.~~O. ***Intrusion Prevention***. All systems involved in accessing, storing, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, ~~must~~shall be protected by an intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. ***System Security Review***.

1. The County Department ~~must~~/Agency shall ensure audit control mechanisms are in place.

2. All systems processing and/or storing Medi-Cal PII ~~must~~shall have at

least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.

3. Reviews should include vulnerability scanning tools.

B. ***Log Reviews***. All systems processing and/or storing Medi-Cal PII ~~must~~shall have a process or automated procedure in place to review system logs for unauthorized access.

C. ***Change Control***. All systems processing and/or storing Medi-Cal PII ~~must~~shall have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. ***Anomalies***. When the ~~county~~County Department/Agency or DHCS suspects MEDS usage anomalies, the ~~county will~~County Department/Agency shall work with DHCS to investigate the anomalies and report conclusions of such investigations and remediation to DHCS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. ***Emergency Mode Operation Plan***. The County Department ~~must~~/Agency shall establish a documented plan to enable continuation of critical business processes and protection of the security of Medi-Cal PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours. It is recommended that counties conduct periodic disaster recovery testing, including connectivity exercises conducted with DHCS, if requested.

B. ***Data Centers***. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of Medi-Cal PII, ~~must~~shall include environmental protection such as cooling~~,~~; power~~,~~; and fire prevention, detection, and suppression; and appropriate protection from other threats, including but not limited to flood, earthquake, and terrorism.

C. ***Data Backup Plan***.

1. The County Department/Agency shall have established documented procedures to backup Medi-Cal PII to maintain retrievable exact copies of Medi-Cal PII.

2. The documented backup procedures shall contain a schedule which includes incremental and full backups.

3. The procedures shall include storing backups containing Medi-Cal PII offsite.

4. The procedures shall ensure an inventory of backup media. It is recommended that the ~~county~~County Department/Agency periodically test the data recovery process.

IX. PAPER DOCUMENT CONTROLS

A. ***Supervision of Data***. Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles***. The County Department/Agency shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. ~~A County that chooses to permit its County Workers to leave records unattended in vehicles must include provisions in its policies to provide the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit Medi-~~A County~~Cal PII~~ Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit Medi-Cal PII to be left unattended in a vehicle overnight or for other extended periods of time.

C. ***Public Modes of Transportation***. Medi-Cal PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., ~~including~~inclusive of baggage areas. This should be included in training due to the nature of the risk.

D. ***Escorting Visitors***. 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.

E. ***Confidential Destruction***. Medi-Cal PII ~~must~~shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data***. Medi-Cal PII ~~must~~shall not be removed from the premises of County Department/Agency except for justifiable business purposes.

G. ***Faxing***.

1. Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas.

2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.

3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. ***Mailing***.

1. Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.

2. Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the County Department/Agency agrees to implement reasonable systems for the discovery and prompt reporting of any ~~Breach~~breach or ~~Security Incident~~security incident, and to take the following steps:

A. ***Initial Notice to DHCS***:

~~**Immediately upon discovery** of a suspected security incident that involves data provided to DHCS by the SSA, the county~~The County Department/Agency shall notify DHCS, by email, or alternatively, by telephone~~.~~

~~**Within one working day of discovery**, the county shall notify DHCS by~~ if email ~~or telephone of unsecured PHI or PI, if that PHI or PI was, or~~ is~~, reasonably believed to have been accessed or acquired by an unauthorized person,~~ unavailable, of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII ~~in violation of this Agreement,~~ or potential loss of ~~confidential~~Medi-Cal PII. When making notification, the following applies:

1. If a suspected security incident involves Medi-Cal PII provided or verified by SSA, the County Department/Agency shall **immediately** notify DHCS upon discovery. *For more information on SSA data~~ affecting~~, please see the Definition section of this Agreement.*

2. If a suspected security incident does not involve Medi-Cal PII provided or verified by SSA, the County Department/Agency shall notify DHCS **within one working day** of discovery.

If it is unclear if the security incident involves SSA data, the County Department/Agency shall immediately report the incident upon discovery.

A County Department/Agency shall notify DHCS of all personal information, as defined by California Civil Code Section 1798.3(a), that may have been accessed, used, or disclosed in any suspected security incident or breach, including but not limited to case numbers.

Notice shall be made using the "DHCS Privacy Incident Report" (PIR) form, including all information known at the time. The County Department/Agency shall use the most current version of this form, which is posted available on the DHCS Privacy Office website (, select "Privacy & HIPAA" and then "County Use") or use this link at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx. Initial, Investigation, and Completed All PIRs and supporting documentation are to be submitted to the DHCS Privacy Office and the DHCS Information via email using the "DHCS Breach and Security Office Incidents Reporting" contact information found below in Subsection F.

A breach shall be treated as discovered by the County Department/Agency as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the County Department. Notice shall be provided to the DHCS Privacy Office and the DHCS Information Security Office.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, the County Department/Agency shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach occurrence and to protect the operating environment; and

2. Any action pertaining to such unauthorized disclosure occurrence required by applicable Federal and State laws and regulations.

B. ***Investigation and Investigative Report***. The county County Department/Agency shall immediately investigate breaches and security incidents involving Medi-Cal PII, and, if the initial PIR did not include all of the information marked with an asterisk, or if new or updated information

is available, submit an updated PIR **within 72 hours of the discovery**. The updated PIR shall include all of the information marked with an asterisk, and all other applicable information listed on the form, to the extent known at that time. Medi-Cal PII. If the initial PIR was submitted incomplete and if new or updated information is available, submit an updated PIR to DHCS **within 72 hours of the discovery**. The updated PIR shall include any other applicable information related to the breach or security incident known at that time.

C. ***Complete Report***. If all of the required information was not included in either the initial report, or the investigation reportPIR submission, then a separate complete report mustshall be submitted **within ten working days of the discovery**. The Complete Report of the investigation shall include an assessment of all known factors relevant to athe determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA, the), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the HIPAA regulations and/Information Protection Act, or stateother applicable law. The report shall also include a fullCAP that shall include, at minimum, detailed corrective action plan, including information onregarding the mitigation measures that were taken to halt and/or contain the improper use or disclosure.

If DHCS requests additional information in additionrelated to that listed on the PIRincident, the County Department/Agency shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised the County Department/Agency shall submit an updated PIR with revisions and/or additional information after the Completed Report is submitted, by submitting the revised or additional information on an updated PIR.has been provided. DHCS will review and approve or disapprove the determination ofdetermine whether a breach occurred, and ifwhether individual notifications and corrective action plans are notification is required. DHCS will maintain the final decision making over a breach determination

D. ***Notification of Individuals.*** When applicable state or federal law requires DHCSnotification to notify individuals of a breach or unauthorized disclosure of their Medi-Cal PII, the County Department/Agency shall give the notice, subject to the following provisions apply: :

1. If the cause of the breach is attributable to the County Department/Agency or its subcontractors, agents or vendors, the County Department/Agency shall pay any costs of such notifications, as well as any and all costs associated with the breach. Theif the cause of the breach is attributable to DHCS, DHCS shall pay any costs associated with such notifications, as well as any costs associated with the breach.

If there is any question as to whether DHCS or the County Department/Agency is responsible for the breach, DHCS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs;

2. All notifications (regardless of breach status) regarding beneficiaries' Medi-Cal PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 1798.29, and 42 U.S.C. section 17932, and of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than **60 calendar days**. from discovery;

1.3. The DHCS Privacy Office shall approve the time, manner and content of any such notifications and their review and approval must be obtained before notifications are made. DHCS may elect to assign responsibility for such notification to the County Department. In the event DHCS assigns notification responsibility to the County Department, DHCS shall provide the County Department with the appropriate direction and procedures to ensure notice is provided pursuant to applicable law. If the cause of the breach is attributable to DHCS, DHCS shall pay any costs associated with such notifications. If there is any question as to whether DHCS or the County Department is responsible for the breach, DHCS and the County Department shall jointly determine responsibility for purposes of allocating the costs of such notices.shall be obtained before notifications are made. If notifications are distributed without DHCS review and approval, secondary follow-up notifications may be required; and

4. DHCS may elect to assume responsibility for such notification from the County Department/Agency.

B. ***Responsibility for Reporting of Breaches when Required by State or Federal Law.*** If the cause of a breach of Medi-Cal PII is attributable to the County Department/Agency or its agents, subcontractors or vendors, the County Department/Agency is responsible for all required reporting the breach and all costs associated withof the breach. If the cause of the breach is attributable to DHCS, DHCS is responsible for all required reporting of the breach and for all costs associated with the

~~B.~~E. ~~breach~~. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS and the County Department/Agency shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

~~C.~~F. ***DHCS Contact Information***. ~~To direct communications to the above-referenced DHCS staff, the~~The County Department/Agency shall ~~initiate contact as indicated herein.~~utilize the below contact information to direct all notifications of breach and security incidents to DHCS. DHCS reserves the right to make changes to the contact information ~~below~~ by giving written notice to the County Department/Agency. Said changes shall not require an amendment to this Agreement ~~to~~or any other agreement into which it is incorporated.

DHCS Breach and Security Incident Reporting
Department of Health Care Services Office of HIPAA Compliance 1501 Capitol Avenue, MS 4721 P.O. Box 997413 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (866) 866-0602 *The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.*

XI. DHCS PSA CONTACTS

The County Department/Agency shall utilize the below contact information for any PSA-related inquiries or questions. DHCS reserves the right to make changes to the contact information by giving written notice to the County Department/Agency. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated. *Please use the contact information listed in Section X of this Agreement for any Medi-Cal PII incident or breach reporting.*

PSA Inquires and Questions
Department of Health Care Services Medi-Cal Eligibility Division 1501 Capitol Avenue, MS 4607 P.O. Box 997417 Sacramento, CA 95899-7417 Email: countypsa@dhcs.ca.gov

XI.XII. COMPLIANCE WITH SSA AGREEMENT

The County Department/Agency agrees to comply with substantiveapplicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS) and), in the Agreement between SSA and DHCS, known as the Information Exchange Agreement (IEA), which are appended and hereby incorporated in to this Agreement (Exhibit A). The specific sections of the IEA with substantive privacy and security requirements, which are to be complied with by the County Department are in the following sections: E, Security Procedures; F, Contractor/Agent Responsibilities; G, Safeguarding and Reporting Responsibilities for PII, and in Attachment 4,) between SSA and DHCS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies

Exchanging Electronic Information with SSA. (TSSR), which are hereby incorporated into this Agreement (Exhibit A) and available upon request.

If there is any conflict between a privacy and security standard in these sections of the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi--Cal PII.

If SSA changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to County Welfare Directors Association (CWDA) as well as the DHCS proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the thirty (30) day period, DHCS will submit the proposed target date to SSA, which will be subject to adjustment by SSA. Once a target date for compliance is determined by SSA, DHCS will supply copies of the changed agreement to the CWDA and the CountiesCounty Departments/Agency, along with the compliance date expected by SSA. If athe County Department/Agency is not able to meet the SSA compliance date, it mustshall submit Corrective Action Plan (a CAP) to DHCS for review and approval at least thirty (30) days prior to the SSA compliance date. Any potential

County Department/Agency resource issues may be discussed with DHCS through a collaborative process in developing their CAP.

A copy of Exhibit A can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section XI of this Agreement.

XII.XIII. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County Department/Agency agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) Betweenbetween the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and the California Department of Health Care Services (CA-DHCS), known as the CMA, which is appended and hereby incorporated in tointo this Agreement (Exhibit B).) and available upon request. If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

If DHS-USCIS changes the terms of its agreement(s) with DHCS, DHCS will, as soon as reasonably possible after receipt, supply copies to CWDA as well as the DHCS proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA on the proposed target date and make adjustments, if appropriate. After the 30-day period, DHCS will submit the proposed target date to DHS-USCIS, which will be subject to adjustment by DHS-USCIS. Once a target date for compliance is determined by DHS-USCIS, DHCS will supply copies of the changed agreement to the CWDA and the Counties, along with the compliance date expected by DHS-USCIS. If a County is not able to meet the DHS-USCIS compliance date, it must

DHCS will supply copies of the changed agreement to the CWDA and the County Department/Agency, along with the compliance date expected by DHS-USCIS. If the County Department/Agency is not able to meet the DHS-USCIS compliance date, it shall submit Corrective Action Plan (a CAP) to DHCS for review and approval at least thirty (30) days prior to the DHS-USCIS compliance date. Any potential County Department/Agency resource issues may be discussed with DHCS through a collaborative process in developing their CAP.

A copy of Exhibit B can be requested by authorized County Department/Agency individuals from DHCS using the contact information listed in Section XI of this Agreement.

~~XIII.~~XIV. COUNTY DEPARTMENT'S/AGENCY'S AGENTS ~~AND~~, SUBCONTRACTORS, AND VENDORS

The County Department/Agency agrees to enter into written agreements with ~~any~~all agents, ~~including~~ subcontractors and vendors~~,~~ that have access to ~~whom County Department provides Medi-Cal PII received from or created or received by~~ County Department ~~in performing functions or activities related to the administration of Medi-Cal that~~ /Agency Medi-Cal PII. These agreements will impose, at a minimum, the same restrictions and conditions ~~on~~that apply to the County Department/Agency with respect to Medi-Cal PII upon such agents, subcontractors, and vendors ~~that apply to the County Department with respect to Medi-Cal PII, including~~.
These shall include, (1) restrictions on disclosure of Medi-Cal PII ~~and~~, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect ~~such~~ Medi-Cal PII~~. The County Department shall incorporate, when applicable, the~~, and, where relevant ~~provisions of this Agreement into each subcontract or subaward to such agents, subcontractors and vendors, including~~, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII be reported to the County Department/Agency. If the agents, subcontractors, and vendors of County Department/Agency access data provided to DHCS and/or CDSS by SSA or DHS-USCIS, the County Department/Agency shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors. If the County Department/Agency executed the HIPAA Amendment with DHCS, the HIPAA Amendment and Exhibit C will need to be incorporated when applicable. County Departments/Agencies who would like assistance or guidance with this requirement are encouraged to contact DHCS via the PSA inbox at CountyPSA@dhcs.ca.gov~~.~~.

~~XIV.~~XV. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the County Department/Agency agrees to ~~allow~~assist DHCS ~~to inspect the~~ in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the County Department/Agency, with reasonable notice from DHCS~~, in order to perform assessments and~~. Such reviews~~. Such inspections~~ shall be scheduled at times that take into account the operational and staffing demands. The County Department/Agency agrees to promptly remedy ~~any violation~~all violations of any provision of this Agreement and certify the same to the DHCS

Privacy Office and DHCS Information Security Office in writing, or to enter into a written ~~corrective action plan~~CAP with DHCS containing deadlines for achieving compliance with specific provisions of this Agreement.

~~XV.~~XVI. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

~~XVI.~~XVII. AMENDMENT OF AGREEMENT

DHCS and the County Department/Agency acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. Upon request by DHCS, the County Department/Agency agrees to promptly enter into negotiations with DHCS concerning an amendment to this Agreement as may be needed by developments in federal and state laws and regulations. In addition to any other lawful remedy, DHCS may terminate this Agreement upon ~~thirty (~~30~~)~~ days written notice if the County Department/Agency does not promptly agree to enter into negotiations to amend this Agreement when requested to do so, or does not enter into an amendment that DHCS deems necessary.

~~XVII.~~XVIII. TERMINATION

A. This Agreement shall terminate on September 1, ~~2019~~2022, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement; ~~county~~through an executed written amendment. County Department/Agency requests for an extension ~~must~~shall be justified ~~to~~ and ~~accepted~~approved by DHCS and limited to no more than a ~~three~~ six (6) month extension. ~~Such an extension may, upon county request and DHCS approval, be renewed for one additional three month period. Regardless of the extension status, all~~

B. **Survival:** All provisions of this Agreement that provide restrictions on disclosures of Medi-Cal PII and that provide administrative, technical, and physical safeguards for the Medi-Cal PII in the County ~~Department's~~ Department/Agency's

possession shall continue in effect beyond the termination or expiration of ~~the~~this Agreement, and shall continue until the Medi-Cal PII is destroyed or returned to DHCS.

~~XVIII.~~XIX. TERMINATION FOR CAUSE

Upon DHCS' knowledge of a material breach or violation of this Agreement by the County Department/Agency, DHCS may provide an opportunity for the County Department/Agency to cure the breach or end the violation and may terminate this Agreement if the County Department/Agency does not cure the breach or end the violation within the time specified by DHCS. This Agreement may be terminated immediately by DHCS if the County Department/Agency has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department ~~must~~/Agency shall return or destroy all Medi-Cal PII in accordance with Section VII, above. The provisions of this Agreement governing the privacy and security of the Medi-Cal PII shall remain in effect until all Medi-Cal PII is returned or destroyed and DHCS receives a certificate of destruction.

~~XIX.~~XX. 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. The contract is effective on ~~the day the final signature is obtained~~September 1, 2019.

For the County of _____ _____,

Department/Agency of _____ ,

_____	_____
(Signature)	(Date)
_____	_____
(Name)	(Title)

For the Department of Health Care Services,

_____	_____
(Signature)	(Date)
Jennifer Kent	Director
_____	_____
(Name)	(Title)

~~Exhibit A~~

EXHIBIT A

Exhibit A consists of the current versions of the following documents, copies of which can be requested by the County Department/Agency information security and privacy staff from DHCS by using the contact information listed in Section XI of this Agreement.

- Computer Matching and Privacy Protection Act Agreement between the SSA and ~~CHHS, and~~ California Health and Human Services Agency
- Information Exchange Agreement between SSA and DHCS ~~with Attachment "~~
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with ~~SSA." These are sensitive documents that are provided separately to the County's privacy and security officer.~~the SSA (TSSR)

~~Exhibit B~~

EXHIBIT B

Exhibit B consists of the current version of the following document, a copy of which can be requested by the County Department/Agency information security and privacy staff from DHCS by using the contact information listed in Section XI of this Agreement.

- Computer Matching Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and ~~The~~ California Department of Health Care Services (~~CA-~~DHCS~~). This is a sensitive document that is provided separately to the County's privacy and security officer.~~)