MEDI-CAL PRIVACY AND SECURITY AGREEMENT

BETWEEN

the California Department of Health Care Services and the

County of Sonoma,

Department/Agency of
Human Services.

PREAMBLE

The Department of Health Care Services (DHCS) and the

County of Sonoma,

Department/Agency of Human Services
(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 Sonoma,

Department/Agency of Human Services
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 the amount of 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. An agent is a person or organization authorized to act on behalf of the County Department/Agency.

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.

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 California Statewide Automated Welfare System (CalSAWS) 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).

AGREEMENTS

DHCS and County Department/Agency mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. County Department/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 431.302 of Title 42 Code of Federal Regulations, as limited by this Agreement, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of a Medi-Cal client, such as through an authorized release of information form, 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. While DHCS is a covered entity under the federal Health Insurance Portability and Accountability Act, as amended from time to time (HIPAA), the County Department/Agency is not required to be the business associate of DHCS, if the activities of the County Department/Agency are limited to determining eligibility for, or enrollment in, Medi-Cal (45 CFR 160.103). Nevertheless, it is the intention of the parties to protect the privacy and security of Medi-Cal PII and the rights of Medi-Cal applicants and beneficiaries in a manner that is consistent with HIPAA and other laws that are applicable. It is not the intention of the parties to voluntarily subject the County Department/Agency to federal HIPAA jurisdiction where it would not otherwise apply, and DHCS does not assert any authority to do so.

1. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to Medi-Cal PII covered under this Agreement beyond those provided through HIPAA, as applicable, County Department/Agency shall:

    a. Comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

    b. Treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section VIII. of this Agreement. It is not the intention of the parties that this subsection I.B.(1)(b) expands the definitions of breach nor security incident set forth this Agreement unless the additional and/or more protective standard has a different definition

for these terms, as applicable.

Examples of laws that provide additional and/or stricter privacy protections to certain types of Medi-Cal PII include, but are not limited to the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

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;

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 five 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 five years.

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.

The periodic privacy and security reviews 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.

B. Utilize Medi-Cal Eligibility Data System (MEDS) audit reports provided by DHCS and other system auditing tools available to County Department/Agency to perform quality assurance and management oversight

reviews of their County Workers' access to Medi-Cal and SSA PII within data systems utilized, including MEDS. For additional information see Medi-Cal Eligibility Division Information Letter | 21-34. Any instances of suspected security incidents or breaches are to be reported to DHCS immediately following the instructions within Section X of this Agreement.

To ensure a separation of duties, these system audit reviews shall be performed by privacy and security staff who do not have access to Medi-Cal PII within the systems. SSA requires DHCS to enforce a separation of duties, excluding any individual who uses MEDS to make benefit or entitlement determinations from participating in oversight, monitoring, or quality assurance functions. DHCS acknowledges that in smaller counties the separation of duties requirement might create a hardship based on there being a small number of people available to perform various tasks. Requests for hardship exemptions will be approved on a case-by-case basis.

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 IX of this Agreement. Any changes to this information should be reported to DHCS within ten days.

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

V. TECHNICAL SECURITY CONTROLS

The State of California Office of Information Security (OIS) and SSA have adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy controls for Information Systems and Organizations, and NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.

OIS and SSA require organizations to comply and maintain the minimum standards outlined in NIST SP 800-53 when working with PII and SSA data. County Department/Agency shall, at a minimum, implement an information security program that effectively manages risk in accordance with the Systems Security Standards and Requirements outlined in this Section of this Agreement.

Guidance regarding implementation of NIST SP 800-53 is available in the Statewide Information Management Manual (SIMM), SIMM-5300-A, which is hereby incorporated into this Agreement (Exhibit C) and available upon request.

DHCS and CDSS will enter into a separate PSA with California Statewide Automated Welfare System (CalSAWS) Joint Powers Authority specific to the CalSAWS. Any requirements for data systems in this PSA would only apply to County Department/Agency's locally operated/administered systems that access, store, or process Medi-Cal PII.

A. Systems Security Standards and Requirements

1. **Access Control (AC)**

Control Number	AC-1
Title	Access Control Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to designated organization officials: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access control controls; b. Review and update the current access control procedures with the organization-defined frequency.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AC-2
Title	Account Management
DHCS Requirement	The organization must: a. Identify and select the accounts with access to Medi-Cal PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access
	authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit Medi-Cal PII based on valid access authorization, need-to-know permission or under the authority to re-disclose Medi-Cal PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
Supplemental Guidance (from NIST 800-53)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Control Number	AC-3
Title	Access Enforcement
DHCS Requirement	The organization must: Enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
Supplemental Guidance	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-
Control Number	AC-3(7)
Title	Access Enforcement | Role-Based Access Control
DHCS Requirement	The organization information system must: enforce a role-based access control policy over defined subjects and objects and controls access based upon the need to utilize Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.
Control Number	AC-3(8)
Title	Access Enforcement | Revocation of Access Authorization
DHCS Requirement	The organization must: Enforce a role-based access control over users and information resources that have access to Medi-Cal PII, and control access based upon organization defined roles and users authorized to assume such roles.
Supplemental Guidance (from NIST 800-53)	Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.
Control Number	AC-4
Title	Information Flow Enforcement
DHCS Requirement	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the need for interconnected systems to share Medi-Cal PII to conduct business.
Supplemental Guidance (from NIST 800-53)	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message- filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18

Control Number	AC-5
Title	Separation of Duties
DHCS Requirement	The organization must: a. Separate organization-defined duties of individuals; b. Document separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. *DHCS also requires that the state organization prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.* *Federal requirements and DHCS policy exclude any employee who uses Medi-Cal PII to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.*
Supplemental Guidance (from NIST 800-53)	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.
Control Number	AC-6
Title	Least Privilege
DHCS Requirement	The organization must: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Supplemental Guidance (from NIST 800-53)	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
Control Number	AC-6(1)
Title	Least Privilege | Authorize Access to Security Functions
DHCS Requirement	The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.
Supplemental Guidance (from NIST 800-53)	Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
Control Number	AC-6(7)
Title	Least Privilege | Review Of User Privileges
DHCS Requirement	The organization must: a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
Supplemental Guidance (from NIST 800-53)	The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.
Control Number	AC-7
Title	Unsuccessful Logon Attempts
DHCS Requirement	The organization must: a. Enforce a limit of no fewer than three (3) and no greater than five (5) consecutive invalid logon attempts by a user during an organization-defined time period; and b. Automatically lock the account/node for: an organization-defined time period; or locks the account/node until released by an administrator; or delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
Supplemental Guidance (from NIST 800-53)	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Number	AC-8
Title	System Use Notification
DHCS Requirement	The organization must: a. Displays to users system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. At a minimum, this can be done at initial logon and is not required for every logon.
Supplemental Guidance (from NIST 800-53)	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.
Control Number	AC-11
Title	Session Lock
DHCS Requirement	The organization's information system: a. Prevents further access to the system by initiating a session lock after 15 minutes or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.
Supplemental Guidance (from NIST 800-53)	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.
Control Number	AC-17
Title	Remote Access
DHCS Requirement	The organization must: a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize remote access to the information system prior to allowing such connections.
Supplemental Guidance (from NIST 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

2. **Accountability, Audit, and Risk Management (AR)**

Control Number	AR-3
Title	Privacy Requirements for Contractors and Service Providers
DHCS Requirement	The organization must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.
Supplemental Guidance (from NIST 800-53)	Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

3. Audit and Accountability (AU)

Control Number	AU-1
Title	Audit and Accountability Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit Medi-Cal PII: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Review and update the current: 1. Audit and accountability policy at least triennially; and 2. Audit and accountability procedures at least triennially.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AU-2
Title	Audit Events
DHCS Requirement	The organization must: a. Audit the following events: 1) Viewing Medi-Cal PII stored within the organization's system; 2) Viewing of screens that contain Medi-Cal PII; 3) All system and data interactions concerning Medi-Cal PII. b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Determines that the following events are to be audited within the information system: 1) Viewing Medi-Cal PII stored within the organization's system; 2) Viewing of screens that contain Medi-Cal PII; 3) All system and data interactions concerning Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4

Control Number	AU-11
Title	Audit Record Retention
DHCS Requirement	The organization must retain audit records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Supplemental Guidance (from NIST 800-53)	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.
Control Number	AU-12
Title	Audit Generation
DHCS Requirement	The organization information system must: a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism; b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3
Supplemental Guidance (from NIST 800-53)	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

4. **Awareness and Training (AT)**

Control Number	AT-1
Title	Security Awareness and Training Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to Medi-Cal PII: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy and; 2. Security awareness and training procedures. The training and awareness programs must include: The sensitivity of Medi-Cal PII, The rules of behavior concerning use and security in systems and/or applications processing Medi-Cal PII, The Privacy Act and other Federal and state laws, including but not limited to Section 14100.2 of the Welfare and Institutions Code and Section 431.302 et. Seq. of Title 42 Code of Federal Regulations, governing collection, maintenance, use, and dissemination of information about individuals, The possible criminal and civil sanctions and penalties for misuse of Medi-Cal PII, The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of Medi-Cal PII, The restrictions on viewing and/or copying Medi-Cal PII, The proper disposal of Medi-Cal PII, The security breach and data loss incident reporting procedures, The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code, Social engineering (phishing, vishing and pharming) and network fraud prevention.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, tandards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Number	AT-2
Title	Security Awareness Training
DHCS Requirement	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.
Control Number	AT-3
Title	Role-Based Security Training
DHCS Requirement	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.
Control Number	AT-4
Title	Security Training Records
DHCS Requirement	The organization must: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for 5 years. SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
Supplemental Guidance (from NIST 800-53)	Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

5. **Contingency Planning (CP)**

Control Number	CP-2
Title	Contingency Plan
DHCS Requirement	The organization must: a. Develop a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by a senior manager; b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the information system at least annually; e. Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

6. **Data Minimization and Retention (DM)**

Control Number	DM-2
Title	Data Retention and Disposal
DHCS Requirement	The organization must: a. Retain each collection of Medi-Cal PII no longer than required for the organization's business process or evidentiary purposes; b. Dispose of, destroys, erases, and/or anonymizes the Medi-Cal PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records). .
Supplemental Guidance (from NIST 800-53)	NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

7. **Identification and Authentication (IA)**

Control Number	IA-2
Title	Identification and Authentication (Organizational Users)
DHCS Requirement	The organization's information system must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
Supplemental Guidance (from NIST 800-53)	Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

Control Number	IA-5
Title	Authenticator Management
DHCS Requirement	The organization must manage information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators within organization-defined time period; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
Supplemental Guidance (from NIST 800-53)	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS- 5, PS-6, SC-12, SC-13, SC-17, SC-28.
Control Number	**IA-5(1)**
Title	Authenticator Management | Password-Based Authentication
DHCS Requirement	The information system, for password-based authentication, must: a. Enforces minimum password complexity of requirements for: * case sensitivity (upper and lower case letters), * number of characters (equal to or greater than fifteen characters), * mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type); c. Stores and transmits only cryptographically-protected passwords; d. Enforces password lifetime of at least 180 days; e. Prohibits prior 10 passwords for reuse ; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.
Supplemental Guidance (from NIST 800-53)	This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

8. **Incident Response (IR)**

Control Number	IR-1
Title	Incident Response Policy and Procedures
DHCS Requirement	The organization must: a. Develops, documents, and disseminates to organization-defined personnel or roles: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy with organization-defined frequency; and 2. Incident response procedures with organization-defined frequency. *DHCS and NIST Guidelines encourage agencies to consider establishing incident response teams or identifying individuals specifically responsible for addressing Medi-Cal PII and DHCS data breaches.*
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	**IR-2**
Title	Incident Response Training
DHCS Requirement	The organization must provide incident response training to information system users consistent with assigned roles and responsibilities: a. Within organization-defined time period of assuming an incident response role or responsibility; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.
Control Number	**IR-4**
Title	Incident Handling
DHCS Requirement	The organization must: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Supplemental Guidance (from NIST 800-53)	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Number	IR-8
Title	Incident Response Plan
DHCS Requirement	The organization must: a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of te organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements; c. Review the incident response plan organization-defined frequency; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protect the incident response plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

9. **Media Protection (MP)**

Control Number	MP-2
Title	Media Access
DHCS Requirement	The organization must: Restricts access to Medi-Cal PII to County Workers who require access to Medi-Call PII for purposes of administering the Medi-Cal program or as required for the administration of other public benefit programs.
Supplemental Guidance (from NIST 800-53)	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.
Control Number	MP-6
Title	Media Sanitization
DHCS Requirement	The organization must: a. Sanitize media containing Medi-Cal PII prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
Supplemental Guidance (from NIST 800-53)	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

10. **Personnel Security (PS)**

Control Number	PS-3
Title	Personnel Screening
DHCS Requirement	The organization must: a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
Control Number	PS-4
Title	Personnel Termination
DHCS Requirement	The organization, upon termination of individual employment, must: a. Disable information system access; b. Terminate/revoke any authenticators/credentials associated with the individual; c. Conduct exit interviews, as needed; d. Retrieve all security-related organizational information system-related property; e. Retain access to organizational information and information systems formerly controlled by terminated individual; and f. Notified organization-defined personnel upon termination.
Supplemental Guidance (from NIST 800-53)	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.
Control Number	PS-6
Title	Access Agreements
DHCS Requirement	The organization must: a. Develop and document access agreements for organizational information systems; b. Reviews and updates the access agreements at organization-defined frequency; and c. Ensure that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency. DHCS requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain Medi-Cal PII.
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Number	PS-7
Title	Third-Party Personnel Security
DHCS Requirement	The organization must: a. Establishes personnel security requirements including security roles and responsibilities for county agents, subcontractors, and vendors; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period; and e. Monitors provider compliance. *The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to Medi-Cal PII. 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.* *The county department/agency must retain the non-disclosure agreements for at least five (5) to seven (7) years for all contractors and agents who processes, views, or encounters Medi-Cal PII as part of their duties*
Supplemental Guidance (from NIST 800-53)	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.
Control Number	PS-8
Title	Personnel Sanctions
DHCS Requirement	The organization must: a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notify organization personnel within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. *If a member of the county's workforce, as defined at 45 CFR 160.103 and inclusive of an employee, contractor, or agent is subject to an adverse action by the organization (e.g., reduction in pay, disciplinary action, termination of employment, termination of contract for services), DHCS recommends the organization remove his or her access to Medi-Cal PII in advance of the adverse action to reduce the possibility that will the individual will perform unauthorized activities that involve Medi-Cal PII, if applicable.*
Supplemental Guidance (from NIST 800-53)	Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

11. Physical and Environmental Protection (PE)

Control Number	PE-3
Title	Physical Access Control
DHCS Requirement	The organization must: a. Enforce physical access authorizations at entry and exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintain physical access audit logs for entry and exit points; c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escort visitors and monitors visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory physical access devices; and g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated
Supplemental Guidance (from NIST 800-53)	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.
Control Number	PE-6
Title	Monitoring Physical Access
DHCS Requirement	The organization must: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and c. Coordinates results of reviews and investigations with the organizational incident response capability.
Supplemental Guidance (from NIST 800-53)	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

12. Planning (PL)

Control Number	PL-1
Title	Security Planning Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to Medi-Cal PII: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy; and 2. Security planning procedures.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies,
	standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	PL-2
Title	System Security Plan
DHCS Requirement	The organization must: a. Develop a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities; c. Review the security plan for the information system; d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protect the security plan from unauthorized disclosure and modification. *Organization's security plan should include detailed information specific to safeguarding Medi-Cal PII.*
Supplemental Guidance (from NIST 800-53)	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

13. Risk Assessment (RA)

Control Number	RA-1
Title	Risk Assessment Policy and Procedures
DHCS Requirement	The organization must: a. Develop, document, and disseminate to system owners using Medi-Cal PII: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	RA-3
Title	Risk Assessment
DHCS Requirement	The organization must: a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in a risk assessment report or organization defined risk report document. c. Review risk assessment results annually; and e. Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Supplemental Guidance (from NIST 800-53)	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM- 9.

Control Number	RA-5
Title	Vulnerability Scanning
DHCS Requirement	The organization must: a. Scan for vulnerabilities in the information system and hosted applications at a minimum of a monthly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; a. Analyze vulnerability scan reports and results from security control assessments; b. Remediate legitimate vulnerabilities within organization defined time periods in accordance with an organizational assessment of risk; and c. Share information obtained from the vulnerability scanning process and security control assessments with all impacted system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Supplemental Guidance (from NIST 800-53)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

14. Security Assessment and Authorization (CA)

Control Number	CA-2
Title	Security Assessments
DHCS Requirement	The organization must: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation with organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to organization-defined individuals or roles.
Supplemental Guidance (from NIST 800-53)	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Control Number	CA-3
Title	System Interconnections
DHCS Requirement	The organization must: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].
Supplemental Guidance (from NIST 800-53)	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.
Control Number	CA-7
Title	Continuous Monitoring
DHCS Requirement	The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes: a. Establishment of Medi-Cal PII security controls to be monitored; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of Medi-Cal PII security controls in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to organization-defined personnel or roles and to DHCS when requested.
Supplemental Guidance (from NIST 800-53)	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Control Number	CA-8
Title	Penetration Testing
DHCS Requirement	The organization must conduct penetration testing annually on systems storing, processing, or transmitting Medi-Cal PII.
Supplemental	Penetration testing is a specialized type of assessment conducted on information systems or
Guidance (from NIST 800-53)	individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

15. System and Communications Protection (SC)

Control Number	SC-7
Title	Boundary Protection
DHCS Requirement	The organization information system must: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Supplemental Guidance (from NIST 800-53)	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on
	protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.
Control Number	**SC-8**
Title	Transmission Confidentiality and Integrity
DHCS Requirement	The organization information system must: Protect the confidentiality of transmitted information.
Supplemental Guidance (from NIST 800-53)	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Number	**SC-8(1)**
Title	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
DHCS Requirement	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
Supplemental Guidance (from NIST 800-53)	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.
Control Number	SC-13
Title	Cryptographic Protection
DHCS Requirement	The organization information system must implement FIPS 140-3 compliant encryption modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Supplemental Guidance (from NIST 800-53)	Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
Control Number	SC-28
Title	Protection of Information at Rest
DHCS Requirement	The organization information system must: Protect the confidentiality of Medi-Cal PII at rest.
Supplemental Guidance (from NIST 800-53)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

16. System and Information Integrity (SI)

Control Number	SI-2
Title	Flaw Remediation
DHCS Requirement	The organization must: a. Identify, report, and correct information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.
Supplemental Guidance (from NIST 800-53)	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.
Control Number	SI-3
Title	Malicious Code Protection
DHCS Requirement	The organization must: a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the information system and real-time scans of files from external sources at the endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
Supplemental Guidance (from NIST 800-53)	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Number	SI-4
Title	Information System Monitoring
DHCS Requirement	The organization must: a. Monitor the information system to detect: 1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the information system through organization-defined techniques and methods; c. Deploy monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; Relevant risk would apply to anything impacting the confidentiality integrity or availability of the information system. f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides organization-defined information system monitoring information to organization-defined personnel and DHCS as needed.
Supplemental Guidance (from NIST 800-53)	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Number	SI-4(5)
Title	Information System Monitoring | System Generated Alerts
DHCS Requirement	The information system alerts County Worker when the following indications of compromise or potential compromise occur 1. Protected system files or directories have been modified without notification from the appropriate change/configuration management channels. 2. System performance indicates resource consumption that is inconsistent with expected operating conditions. 3. Auditing functionality has been disabled or modified to reduce audit visibility. 4. Audit or log records have been deleted or modified without explanation. 5. The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition. 6. Resource or service requests are initiated from clients that are outside of the expected client membership set. 7. The system reports failed logins or password changes for administrative or key service accounts. 8. Processes and services are running that are outside of the baseline system profile. 9. Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
Supplemental Guidance (from NIST 800-53)	Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.
Control Number	SI-4(13)
Title	Information System Monitoring | Analyze Traffic / Event Patterns
DHCS Requirement	The organization must: a. Analyzes communications traffic/event patterns for the information system; b. Develops profiles representing common traffic patterns and/or events; and c. Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
Supplemental Guidance (from NIST 800-53)	None

17. System and Services Acquisition (SA)

Control Number	SA-9
Title	External Information System Services
DHCS Requirement	The organization must: a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with DHCS PSA, applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. *The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of Medi-Cal PII to such contractors and agents. Prior to signing the Agreement, and thereafter at DHCS's request, the state organization will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to Medi-Cal PII and provide such lists to DHCS.*
Supplemental Guidance (from NIST 800-53)	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Number	SA-11
Title	Developer Security Testing And Evaluation
DHCS Requirement	The organization must require the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

B. Minimum Cloud Security Requirements

County Department/Agency and any agents, subcontractors, and vendors storing Medi-Cal PII in a cloud service must comply with the Cloud Computing Policy, State Administration Manual (SAM) Sections 4983-4983.1, and employ the capabilities in the Cloud Security Standard, SIMM 5315-B to protect information and systems in cloud services as outlined below.

1. Identify and classify assets to focus and prioritize efforts in aligning business needs and risk management.
2. Each information asset for which the County Department/Agency entity has ownership responsibility shall be inventoried and identified to include the following:
    a. Description and value of the information asset.
    b. Owner of the information asset.
    c. Custodians of the information asset.
    d. Users of the information asset.
    e. Classification of information.
    f. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).
    g. Importance of information assets to the execution of the Agency/state entity's mission and program function.
    h. Potential consequences and impacts if confidentiality, integrity, and availability of the information asset were compromised.

3. Security of cloud services stems from managing authentication and fine-grained authorization. To safeguard cloud systems, County Department/Agency shall establish processes and procedures to ensure:
    a. Maintenance of user identities, including both provisioning and de-provisioning;
    b. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
    c. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
    d. Separation of duties to avoid functional conflicts;
    e. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
    f. Use of privileged accounts that can bypass security are restricted and audited;
    g. Systems to administer access based on roles are defined and installed; and
    h. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

4. Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities. PaaS and SaaS resources may already have these controls implemented by the service provider. County Department/Agency must configure information assets to provide only

essential capabilities.

5. County Department/Agency are entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed data storage services with native protection and backup features, but these features must be configured and managed appropriately.
6. Detective controls identify potential security threats or incidents, supporting timely investigation and response. County Department/Agency must continuously identify and remediate vulnerabilities.
7. Response controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. Compliance with incident management requirements as outlined in VII. Notification and Investigation of Breaches and Security Incidents.
8. Recover controls facilitate long-term recovery activities following events or incidents. With cloud services, primarily SaaS solutions, the services provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. County Department/Agency must ensure agreements with cloud service providers include recover controls.

C. ***Minimum Necessary.*** Only the minimum necessary amount of Medi-Cal PII required to perform required business functions applicable to the terms of this Agreement may be used, disclosed, copied, downloaded, or exported.

D. ***Transmission and Storage of Medi-Cal PII.*** All persons that will be working with Medi-Cal PII shall employ FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1 encryption of Medi-Cal PII at rest and in motion unless County Department/Agency determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, County Department/Agency shall maintain, at a minimum, the most current industry standards for transmission and storage of DHCS data and other confidential information.

E. ***DHCS Remote Work Policy.*** County Department/Agency, its County Workers and any agents, subcontractors, and vendors accessing Medi-Cal PII pursuant to this PSA when working remotely, shall follow reasonable policies and procedures that are equivalent to or better than the DHCS Remote Work Policy, as published in Medi-Cal Eligibility Division Informational Letter (MEDIL) | 23-35E. Working remotely means working from a physical location not under the control of the person's employer.

If DHCS changes the terms of the DHCS Remote to Work Policy, DHCS will, as soon as reasonably possible, supply copies to CWDA and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from

CWDA and the County Department/Agency or its designee on the proposed changes. DHCS will issue a new policy in a future MEDIL. If the County Department/Agency is unable to comply with these standards, the CWD will be asked to develop a Plan of Action and Milestones (POA&M) detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to DHCS for review and approval. Any CWDA who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

VI. AUDIT CONTROLS

A. ***Audit Control Mechanisms.*** The County Department/Agency shall ensure audit control mechanisms are in place that are compliant with the Technical Security Controls within Section V of this Agreement..

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

C. ***Notification to DHCS in event County Department/Agency is subject to other Audit.*** If County Department/Agency is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of law related to the privacy and security of PII, including but not limited to Medi-Cal PII, the County Department/Agency shall promptly notify DHCS unless it is legally prohibited from doing so.

VII. PAPER, RECORD, AND MEDIA CONTROLS

A. ***Supervision of Data.*** Medi-Cal PII shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office at the individual's place of employment or at home when working remotely. 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 Department/Agency that chooses to permit its County Workers to leave records unattended in vehicles, 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 shall not be left unattended at any time in airplanes, buses, trains, etc., 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 shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data.*** Medi-Cal PII 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.

VIII. 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 or security incident, and to take the following steps:

A. ***Initial Notice to DHCS:***
The County Department/Agency shall notify DHCS using DHCS' online incident reporting portal of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII or potential loss of 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, 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 promptly and in no event later than one working day of discovery of:

    a. Unsecured Medi-Cal PII if the Medi-Cal PII is reasonably believed to have been accessed or acquired by an unauthorized person;
    b. Any suspected security incident which risks unauthorized access to Medi-Cal PII and/or;
    c. Any intrusion or unauthorized access, use, or disclosure of Medi-Cal PII in violation of this Agreement; or
    d. Potential loss of Medi-Cal PII affecting this Agreement.

Notice to DHCS shall include all information known at the time the incident is reported. The County Department/Agency can submit notice via the DHCS incident reporting portal which is available online at: https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx

If DHCS' online incident reporting portal is unavailable, notice to DHCS can instead be made via email using the DHCS Privacy Incident Report (PIR) form. The email address to submit a PIR can be found on the PIR and in subsection H of this section. The County Department/Agency shall use the most current version of the PIR, which is available online at: https://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf.

If the County Department/Agency is unable to notify DHCS the via the Incident Reporting Portal or email, notification can be made by telephone using the contact information listed in subsection H.

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.

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 security incident or breach; and

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

B. ***Investigation of Security Incident or Breach.*** The County Department/Agency shall immediately investigate such a security incident, breach, or unauthorized use of Medi-Cal PII.

C. ***Complete Report.*** Within ten (10) working days of the discovery the County Department/Agency shall provide any additional information related to the incident requested by DHCS. The County Department/Agency shall make reasonable efforts to provide DHCS with such information.

The complete report must include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable federal and state laws. The report shall include a full, detailed corrective action plan (CAP) including mitigating measures that were taken to halt and/or contain the improper use or disclosure.

If DHCS requests additional information related to the incident, the County Department/Agency shall make reasonable efforts to provide DHCS with such information. If necessary, the County Department/Agency shall submit an updated report with revisions and/or additional information after the Completed Report has been provided. DHCS will review and determine whether a breach occurred and whether individual notification is required. DHCS will maintain the final decision making over a breach determination.

D. ***Notification of Individuals.*** If the cause of a breach is solely attributable to County Department/Agency or its agents, County Department/Agency shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made. DHCS and the County Department/Agency shall work together to ensure that notification of individuals is done in compliance with statutory deadlines within applicable federal and state law.

If the cause of a breach is solely attributable to DHCS, DHCS shall pay all costs of 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 or DHCS and the County Department/Agency acknowledge that both are responsible for the breach, DHCS and the County Department/Agency shall jointly determine responsibility for purposes of allocating the costs.

1. 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 17932 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 **sixty (60) calendar days** from discovery.

E. ***Responsibility for Reporting of Breaches***

1. ***Breach Attributable to County Department/Agency.*** 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 shall be responsible for all required reporting of the breach.

2. ***Breach Attributable to DHCS.*** If the cause of the breach is attributable to DHCS, DHCS shall be responsible for all required reporting of the breach.

F. ***Coordination of Reporting.*** 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 compliant with applicable law and prevent duplicate reporting and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

G. ***Submission of Sample Notification to Attorney General:*** If the cause of the breach is attributable to the County Department/Agency or an agent, subcontractor, or vendor of the County Department/Agency and if notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, regardless of whether County Department/Agency is considered only a custodian and/or non-owner of the Medi-Cal PII, County Department/Agency shall, at its sole expense and at the sole election of DHCS, either:

1. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). County Department/Agency shall inform the DHCS Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or

2. Cooperate with and assist DHCS in its submission of a sample copy of the notification to the Attorney General.

H. ***DHCS Contact Information.*** The County Department/Agency shall utilize the below contact information to direct all communication/notifications of breach and security incidents to DHCS. 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.

DHCS Breach and Security Incident Reporting
Privacy Officer c/o Data Privacy Unit Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (916) 445-4646 *The preferred method of communication is email, when available. Do not include any Medi-Cal PII unless requested by DHCS.*

IX. 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

X. COMPLIANCE WITH SSA AGREEMENT

The County Department/Agency agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CalHHS), in the Information Exchange Agreement (IEA) 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 incorporated into this Agreement within section V. Technical Security Controls and Exhibit A (available upon request).
If there is any conflict between a privacy and security standard in 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) and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA and the County Department/Agency or its designee 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 CWDA and the County Department/Agency or its designee, along with the compliance date expected by SSA. If the County Department/Agency is not able to meet the SSA compliance date,, the County Department/Agency will be asked to develop a POA&M detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to DHCS for review and approval. Any County Department/Agency who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

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.

XI. 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) between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and DHCS, which is hereby incorporated into 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 the CWDA and the County Department/Agency or its designee as well as DHCS' proposed target date for compliance. For a period of thirty (30) days, DHCS will accept input from CWDA and the County Department/Agency or its designee 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 CWDA and the County Department/Agency or its designee, along with the compliance date expected by DHS-USCIS. If the County Department/Agency is not able to meet the DHS-USCIS compliance date, the POA&M must be provided to DHCS for review and approval. Any County Department/Agency who is under a POA&M will be required to provide quarterly updates to DHCS until the fully compliant.

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

XII. COUNTY DEPARTMENT'S/AGENCY'S AGENTS, SUBCONTRACTORS, AND VENDORS

The County Department/Agency agrees to enter into written agreements with all agents, subcontractors and vendors that have access to County Department/Agency Medi-Cal PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the County Department/Agency with respect to Medi-Cal PII upon such agents, subcontractors, and vendors. These shall include, (1) restrictions on disclosure of Medi-Cal PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect Medi-Cal PII, and, where relevant, (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.

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.

XIII. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the County Department/Agency agrees to assist DHCS 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. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The County Department/Agency agrees to promptly remedy 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 POA&M with DHCS containing deadlines for achieving compliance with specific provisions of this Agreement.

XIV. 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.

XV. 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 ensure compliance with such changes. 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 changes in federal and state laws and regulations or NIST 800-53. In addition to any other lawful remedy, DHCS may terminate this Agreement upon 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.

XVI. TERMINATION

This Agreement shall terminate on September 1, 2028, 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 Department/Agency's requests for an extension shall be approved by DHCS and limited to no more than a six (6) month extension.

A. ***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/Agency's possession shall continue in effect beyond the termination or expiration of this Agreement and shall continue until the Medi-Cal PII is destroyed or returned to DHCS.

XVII. 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/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.

XVIII. 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 September 1, 2024.

For the County of Sonoma,

Department/Agency of Human Services,

Angela Struckmann Digitally signed by Angela Struckmann Date: 2024.08.15 09:37:22 -07'00'	8/15/2024
(Signature)	(Date)
Angela Struckmann	Department Director
(Name)	(Title)

For the Department of Health Care Services,

DocuSigned by: Sarah Crow A810D8ECE6C8445...	August 19, 2024
(Signature)	(Date)
Sarah Crow	Medi-Cal Eligibility Division Chief
(Name)	(Title)

DHCS HIPAA Business Associate Addendum

1. This Agreement has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing privacy and security regulations at 45 Code of Federal Regulations, Parts 160 and 164 (collectively, and as used in this Agreement)

2. The term "Agreement" as used in this document refers to and includes both this Business Associate Addendum and the contract to which this Business Associate Agreement is attached as an exhibit, if any.

3. For purposes of this Agreement, the term "Business Associate" shall have the same meaning as set forth in 45 CFR section 160.103.

4. The Department of Health Care Services (DHCS) intends that Business Associate may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute Protected Health Information (PHI) and/or confidential information protected by Federal and/or state laws.

4.1 As used in this Agreement and unless otherwise stated, the term "PHI" refers to and includes both "PHI" as defined at 45 CFR section 160.103 and Personal Information (PI) as defined in the Information Practices Act (IPA) at California Civil Code section 1798.3(a). PHI includes information in any form, including paper, oral, and electronic.

4.2 As used in this Agreement, the term "confidential information" refers to information not otherwise defined as PHI in Section 4.1 of this Agreement, but to which state and/or federal privacy and/or security protections apply.

5. Contractor (however named elsewhere in this Agreement) is the Business Associate of DHCS acting on DHCS's behalf and provides services or arranges, performs or assists in the performance of functions or activities on behalf of DHCS, and may create, receive, maintain, transmit, aggregate, use or disclose PHI (collectively, "use or disclose PHI") in order to fulfill Business Associate's obligations under this Agreement. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."

6. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in HIPAA and/or the IPA. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

7. Permitted Uses and Disclosures of PHI by Business Associate

Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of DHCS, provided that such use or disclosure would not violate HIPAA or other applicable laws if done by DHCS.

7.1 Specific Use and Disclosure Provisions

Except as otherwise indicated in this Agreement, Business Associate may use and disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Business Associate may disclose PHI for this purpose if the disclosure is required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person. The person shall notify the Business Associate of any instances of which the person is aware that the confidentiality of the information has been breached, unless such person is a treatment provider not acting as a business associate of Business Associate.

8. Compliance with Other Applicable Law

8.1 To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, more protective) privacy and/or security protections to PHI or other confidential information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:

8.1.1 To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

8.1.2 To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 18. of this Agreement.

8.2 Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or confidential information, as defined in Section 4. of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

8.3 If Business Associate is a Qualified Service Organization (QSO) as defined in 42 CFR section 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 CFR section 2.11.

9. Additional Responsibilities of Business Associate

9.1 Nondisclosure

9.1.1 Business Associate shall not use or disclose PHI or other confidential information other than as permitted or required by this Agreement or as required by law.

9.2 Safeguards and Security

9.2.1 Business Associate shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards shall be based on applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels.

9.2.2 Business Associate shall, at a minimum, utilize a National Institute of Standards and Technology Special Publication (NIST SP) 800-53 compliant security framework when selecting and implementing its security controls and shall maintain continuous compliance with NIST SP 800-53 as it may be updated from time to time. The current version of NIST SP 800-53, Revision 5, is available online at; updates will be available online through the Computer Security Resource Center website.

9.2.3 Business Associate shall employ FIPS 140-2 validated encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. FIPS 140-2 validation can be determined online through the Cryptographic Module Validation Program Search, with information about the Cryptographic Module Validation Program under FIPS 140-2. In addition, Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

9.2.4 Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other confidential information may be used.

9.2.5 Business Associate shall ensure that all members of its workforce with access to PHI and/or other confidential information sign a confidentiality statement prior to access to such data. The statement must be renewed annually.

9.2.6 Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C.

9.3 Business Associate's Agent

Business Associate shall ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "agents") that use or disclose PHI and/or confidential information on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI and/or confidential information.

10. Mitigation of Harmful Effects

Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI and other confidential information in violation of the requirements of this Agreement.

11. Access to PHI

Business Associate shall make PHI available in accordance with 45 CFR section 164.524.

12. Amendment of PHI

Business Associate shall make PHI available for amendment and incorporate any amendments to protected health information in accordance with 45 CFR section 164.526.

13. Accounting for Disclosures

Business Associate shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR section 164.528.

14. Compliance with DHCS Obligations

To the extent Business Associate is to carry out an obligation of DHCS under 45 CFR Part 164, Subpart E, comply with the requirements of the subpart that apply to DHCS in the performance of such obligation.

15. Access to Practices, Books and Records

Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of DHCS available to DHCS upon reasonable request, and to the federal Secretary of Health and Human Services for purposes of determining DHCS' compliance with 45 CFR Part 164, Subpart E.

16. Return or Destroy PHI on Termination; Survival

At termination of this Agreement, if feasible, Business Associate shall return or destroy all PHI and other confidential information received from, or created or received by Business Associate on behalf of, DHCS that Business Associate still maintains in any form and retain no copies of such information. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

17. Special Provision for SSA Data

If Business Associate receives data from or on behalf of DHCS that was verified by or provided by the Social Security Administration (SSA data) and is subject to an agreement between DHCS and SSA, Business Associate shall provide, upon request by DHCS, a list of all employees and agents and employees who have access to such data, including employees and agents of its agents, to DHCS.

18. Breaches and Security Incidents

Business Associate shall implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

18.1 Notice to DHCS

18.1.1 Business Associate shall notify DHCS immediately upon the discovery of a suspected breach or security incident that involves SSA data. This notification will be provided by email upon discovery of the breach. If Business Associate is unable to provide notification by email, then Business Associate shall provide notice by telephone to DHCS.

18.1.2 Business Associate shall notify DHCS within 24 hours by email (or by telephone if Business Associate is unable to email DHCS) of the discovery of the following, unless attributable to a treatment provider that is not acting as a business associate of Business Associate:

18.1.2.1 Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

18.1.2.2 Any suspected security incident which risks unauthorized access to PHI and/or other confidential information;

18.1.2.3 Any intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement; or

18.1.2.4 Potential loss of confidential information affecting this Agreement.

18.1.3 Notice shall be provided to the DHCS Program Contract Manager (as applicable), the DHCS Privacy Office, and the DHCS Information Security Office (collectively, "DHCS Contacts") using the DHCS Contact Information in Section 18.6.

Notice shall be made using the current DHCS "Privacy Incident Reporting Form" ("PIR Form"; the initial notice of a security incident or breach that is submitted is referred to as an "Initial PIR Form") and shall include all information known at the time the incident is reported. The form is available online at the DHCS Data Privacy webpage.

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, Business Associate shall take:

18.1.3.1 Prompt action to mitigate any risks or damages involved with the security incident or breach; and

18.1.3.2 Any action pertaining to such unauthorized disclosure required by applicable Federal and State law.

18.2 Investigation

Business Associate shall immediately investigate such security incident or breach.

18.3 Complete Report

To provide a complete report of the investigation to the DHCS contacts within ten (10) working days of the discovery of the security incident or breach. This "Final PIR" must include any applicable additional information not included in the Initial Form. The Final PIR Form shall include an assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws. The report shall also include a full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that requested through the PIR form, Business Associate shall make reasonable efforts to provide DHCS with such information. A "Supplemental PIR" may be used to submit revised or additional information after the Final PIR is submitted. DHCS will review and approve or disapprove Business Associate's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and Business Associate's corrective action plan.

18.3.1 If Business Associate does not complete a Final PIR within the ten (10) working day timeframe, Business Associate shall request approval from DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final PIR.

18.4 Notification of Individuals

If the cause of a breach is attributable to Business Associate or its agents, other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate shall notify individuals accordingly and shall pay all costs of such notifications, as well as all costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

18.5 Responsibility for Reporting of Breaches to Entities Other than DHCS

If the cause of a breach of PHI is attributable to Business Associate or its agents, other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate is responsible for all required reporting of the breach as required by applicable federal and state law.

18.6 DHCS Contact Information

To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated here. DHCS reserves the right to make changes to the contact information below by giving written notice to Business Associate. These changes shall not require an amendment to this Agreement.

18.6.1 DHCS Program Contract Manager

See the Scope of Work exhibit for Program Contract Manager information. If this Business Associate Agreement is not attached as an exhibit to a contract, contact the DHCS signatory to this Agreement.

18.6.2 DHCS Privacy Office

Privacy Office
c/o: Office of HIPAA Compliance
Department of Health Care Services
P.O. Box 997413, MS 4722
Sacramento, CA 95899-7413

Email: incidents@dhcs.ca.gov

Telephone: (916) 445-4646

18.6.3 DHCS Information Security Office

Information Security Office
DHCS Information Security Office
P.O. Box 997413, MS 6400
Sacramento, CA 95899-7413

Email: incidents@dhcs.ca.gov

19. Responsibility of DHCS

DHCS agrees to not request the Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

20. Audits, Inspection and Enforcement

20.1 From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. Whether or how DHCS exercises this provision shall not in any respect relieve Business Associate of its responsibility to comply with this Agreement.

20.2 If Business Associate is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Business Associate shall promptly notify DHCS unless it is legally prohibited from doing so.

21. Termination

21.1 Termination for Cause

Upon DHCS' knowledge of a violation of this Agreement by Business Associate, DHCS may in its discretion:

21.1.1 Provide an opportunity for Business Associate to cure the violation and terminate this Agreement if Business Associate does not do so within the time specified by DHCS; or

21.1.2 Terminate this Agreement if Business Associate has violated a material term of this Agreement.

21.2 Judicial or Administrative Proceedings

DHCS may terminate this Agreement if Business Associate is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

22. Miscellaneous Provisions

22.1 Disclaimer

DHCS makes no warranty or representation that compliance by Business Associate with this Agreement will satisfy Business Associate's business needs or compliance obligations. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other confidential information.

22.2 Amendment

22.2.1 Any provision of this Agreement which is in conflict with current or future applicable Federal or State laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it, and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

22.2.2 Failure by Business Associate to take necessary actions required by amendments to this Agreement under Section 22.2.1 shall constitute a material violation of this Agreement.

22.3 Assistance in Litigation or Administrative Proceedings

Business Associate shall make itself and its employees and agents available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Business Associate.

22.4 No Third-Party Beneficiaries

Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

22.5 Interpretation

The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

22.6 No Waiver of Obligations

No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.